Elsag Plate Hunter®

EOC Administrator's Guide

Publication Number MPH-900-OCAM • Version 5.6 • December 2016

Notice
Every effort was made to ensure that the information in this document was accurate at the time of printing or electronic distribution. However, all information is subject to change without notice.

Trademark Information
EOC™ is a trademark of Selex ES Inc.
FPH-900™ is a trademark of Selex ES Inc.
LPRCore™ is a trademark of Selex ES Inc.
Elsag Plate Hunter® is a registered trademark of Selex ES Inc.

Selex ES Contact Information
To contact us, please refer to the information below:

Professional Services
7 Sutton Place
Brewster, NY 10509
Telephone: 866-9-MPH-900 (866-967-4900)
OR
Telephone: 845-278-5425
Facsimile: 845-278-5428

Technology and Manufacturing
205 H Creek Ridge Road
Greensboro, NC 27406
Telephone: 336-379-7135
Facsimile: 336-379-7164

Technical Support Department
Telephone: 866-9-MPH-900 (866-967-4900)
OR
www.elsag.com/contact_form.htm

Visit us on the Internet
www.elsag.com

Ordering Information
The ordering number for this publication is Publication Number MPH-900-OCUM • Version 5.6. To order this document, contact Selex ES Inc.

IMPORTANT: If you are in possession of a printed or electronic version of this user's guide, be aware that it may not be the current version. To ensure that you are using the most up-to-date version of this user's guide, please contact Selex ES Inc.

Table of Contents

List of Figures

List of Tables

1 General Information

1.1 About This Manual

This manual contains information about the Selex ES Inc. Enterprise Operations Center System. It covers the various parameters of the application including instructions for daily operation of the system. The intended audiences for this manual include Selex ES Inc.'s customers' general operating personnel, system administrators, authorized Selex ES Inc. clients and business partners, and Software Product Evaluators. It is primarily focused on the tasks required for day-to-day operation of the system for administrative personnel.

1.2 Revision Information

If it becomes necessary to revise this installation guide, Selex ES Inc. will give the reasons for the revision in this section.

Table A — Manual Revision Information (English Version)

Version	Description	Revised Date	Revised By	Approved By
1.0	First release	June 2012	DC	CT, NW
1.1	Updated	July 2012	DC	CT, NW
1.2	Updated, added cross search, convoy search	September 2012	DC	CT, NW
2.0	Updated, TOC, cross search, convoy search	October 2012	MM	CT, NW
3.0	Updated for EOC 5.0 Release	August 2013	CT	CT, NW
4.0	Updated for EOC 5.2 Release	February 2014	LR, CW	LR, SM
5.3	Updated for EOC 5.3 Release	July 2014	LR	LR, SM
5.4	Updated for EOC 5.4 Release	October 2015	LR	LR, SM
5.5	Updated for EOC 5.5 Release	December 2015	TV	TV, SM
5.6	Updated for EOC 5.6 Release	May 2016	GR	GR,LR.SM
5.6	Updated for EOC Suite 5.6 Parking	December 2016	GR	SM

1.3 Selex ES Terminology, Acronyms, and Terms

The following terms include acronyms that may appear throughout this and other Selex ES Inc. publications; however, they are terms with which a beginning user may not be familiar.

Term	Explanation/Definition/Description
Alarm	A read whose license plate number matches a List entry.
CarSystem	The vehicle or FCU PC application which allows operator interaction with reads, alarms and lists.
CSV	**C**omma-**S**eparated **V**alue
EOC	**E**nterprise **O**peration **C**enter
EPH	**Elsag Plate Hunter**
FCU	**F**ield **C**ontrol **U**nit – Electronic cabinet connected to up to 4 LPR Fixed Cameras and, normally, a computer running the CarSystem application.
GPS	**G**eo **P**ositioning **S**ystem
GUI	**G**raphical **U**ser **I**nterface (pronounced GOO-ee)
IIS	**I**nternet **I**nformation **S**ervices
LAN	**L**ocal **A**rea **N**etwork
List	Any collection of license plate numbers.
LPR	**L**icense **P**late **R**eader or **L**icense **P**late **R**eading
LPRCore	SELEX ES Middleware
MDT	**M**obile **D**ata **T**erminal
MPH	**M**obile **P**late **H**unter
PC	**P**ersonal **C**omputer
Read	The data packet associated with an LPR read event which includes the license plate, GPS location, timestamp, JPEG black and white image of the plate and JPEG color overview of the vehicle.
Reader	Collection of cameras at the same location or in a mobile unit (car).
TOC	**T**actical **O**peration **C**enter (superseded by Dispatcher)
USB	**U**niversal **S**erial **B**us

2 Authentication and Login

2.1 Introduction — Authentication and Login

Once the Selex ES Inc. Enterprise Operations Center is installed, you'll need the following information to log in for the first time:

- The URL of the EOC System, and
- The default username and password.

The default user initially has maximum permissions (set by the default group) within the EOC database; in essence, the default user is a system administrator-level user, able to create domains, groups, and users and perform all administrative tasks.

The EOC system operates in one of two authentication modes: **SQL Server Mode** and **Active Directory Mode**. The primary difference is that in **SQL Server Mode**, authentication is performed by the EOC using data maintained in the SQL Server database. In **Active Directory Mode**, authentication is performed by Windows Active Directory.

The two modes have similar functionality, but the user interface is organized in slightly different ways.

2.2 EOC User Authentication Modes

The EOC system operates in one of two authentication modes: **SQL Server Mode** and **Active Directory Mode**. The mode in which your implementation of EOC operates is set up at installation time. Users with administrator rights can switch an installed EOC between the two modes; see *Changing from SQL Server Mode to Active Directory Mode* on page 85 to learn how.

SQL Server Mode requires an administrator to create users in the EOC user interface, which are stored in the EOC's SQL Server database, and use those accounts to manage login authentication. In essence, the EOC handles user authentication independently of the Microsoft[1] Windows[2] domain network.

Active Directory Mode uses the Microsoft Active Directory[3], a service for Windows domain networks that serves as a central mechanism for network administration and security. In Active Directory mode, the EOC authenticates users using Active Directory, i.e., Windows domain user accounts. That is, the Windows system enforces authentication independently of the EOC.

Note that, although user authentication and management are performed through Windows, administrators will need to set up accounts within the EOC to map to those Windows user accounts. See *Logging in to the EOC — Active Directory Mode* in the *Elsag Plate Hunter EOC User's Guide* for details.

[1] Microsoft® is a registered trademark of Microsoft Corporation.

[2] Windows® is a registered trademark of Microsoft Corporation.

[3] Active Directory® is a registered trademark of Microsoft Corporation.

2.2.1 Active Directory Mode — Differences

There are two significant ways in which Active Directory Mode differs from SQL Server Mode. Both are related to the fact that, in Active Directory Mode, user authentication and user management are performed by the Windows system, not by the EOC.

- The user login screen is slightly different. The user login process in Active Directory Mode is detailed in *Logging in to the EOC — Active Directory* Mode in the *Elsag Plate Hunter EOC User's Guide*.
- Creating and managing users in Active Directory Mode is detailed in *Managing Users — Active Directory Mode* on page 28.

The currently configured user authentication mode also affects how users are authenticated when they log into CarSystem. The rules for user authentication are always the same in CarSystem as they are in EOC.

2.3 Getting Started — Domains, Groups, and Users

Once you've installed the EOC successfully, you must configure the system in the way in which you plan to use it, by creating and editing domains, users, and groups (for more information about how the EOC Security System works, please see *Security System* on page 14.

Domains provide you with a way to categorize data within the EOC server. When you create users and groups, you assign them to a domain. You can also use domains to segregate different kinds of data, such as confidential lists.

Groups control the permissions assigned to the users that belong to that group. Access to data and EOC functionality depends on the permissions assigned by the administrators. For example, if you want some users to be able to perform system configuration tasks, you would create one group with permission to do those tasks within the appropriate domain and another without those permissions. Note that groups can grant privileges in multiple domains.

To configure the EOC, you must perform the following sequence of steps:

- Create one or more domains
- Create a group or groups with permissions on the new domain, and
- Create users and associate them with the group (or groups) to give them appropriate permissions within the EOC.

2.3.1 Default Installed Account, Password, and Permissions

When the EOC is first installed, the default Administrator user is a member of the Administrative group. The Administrative group grants maximum permissions to its members. This makes the Administrator user the system administrator account for the system. The default password for the Administrator user after the EOC is first installed is **defaulteocpassword**.

> **NOTE:** After logging into the EOC for the first time using the Administrator user, you should change the password. Be sure to note the new password and keep it somewhere secure.

You may also use the Administrator user to create new users for your administration team with names of your choosing. You then add those users to the Administrators group to give them administrator rights. Each administrator would then use their own user account to perform all administrative tasks. In this way, all audit messages will show who actually performed the action, instead of the anonymous user Administrator.

2.3.2 Password Parameters and Requirements

If you are operating in SQL Server Mode, your user accounts will have the following restrictions:

- Passwords must be a minimum of six characters in length, using any alphanumeric and/or special characters, and
- Five (5) incorrect login attempts will lock a user out of the system, in which case the system administrator will have to re-enable the account.

NOTE: The time window in which consecutive failed attempts are tracked is ten (10) minutes. Thus, if you try four times and fail, then wait ten minutes, the system will see your next attempt as the first, not the fifth. Password parameters and requirement constraints can be modified using the *SQL Membership Provider* option described on page 67.

If you are operating in Active Directory Mode, the only restrictions on passwords are those enforced by your Windows Active Directory system. There is nothing in the EOC that you can do to change them.

The EOC system's authentication mode is set at install time. Administrators can change the authentication mode at any time. Please see the *Membership Provider: SQL or Active Directory* section on page 81 for instructions.

3 Security System

3.1 Introduction

The three most important administrative tasks in the EOC are:

- Making sure that users can only access the features they are allowed to access,
- Making sure that data is viewed only by the people who are authorized to see it, and
- Making sure that only trusted people can modify that data.

To keep these tasks as simple as possible, a system of domains, groups, privileges and users is used to control data access.

3.2 Domains

Data in the EOC is organized into domains that the administrator creates. Each read, alarm, list, reader, camera, user and group belongs to a domain. Each user can be a member of any number of groups. Groups grant their members access to EOC features and the data in the domains using privileges.

Domains can represent any desired logical grouping of data. For large organizations, domains can represent precincts or municipalities or other geographic areas. Domains can also be used to segregate data for ongoing investigations where access to data must be restricted. Organizations which operate multiple parking lots which allow only registered vehicles to park in them use domains to represent the parking lots. Finally, domains can be used to restrict access to data to only those who need to know it.

A good domain organization scheme that we advise you to consider using is to organize your domains into Data Domains and List Domains. A Data Domain would contain the FCUs, Cars and their associated LPR sites. When reads are received from these sites, the reads are automatically added to the domain that the site belongs to. The List Domains would only contain Lists and their associated license plate entries. Any alarms that are generated from reads are automatically added to the domain that the List belongs to. This configuration makes it easier to control who is able to view the alarm data generated from the Lists.

The domains in your EOC implementation can be set up on any basis you need. Your organization can use any combination of these concepts to create domains. You should design a plan for organizing your data before installation and stick with it.

3.3 Groups

A group represents a collection of users who all share a set of privileges. When you create a group, you assign it a set of privileges for some or all EOC features as well as access to some or all domains within the EOC database. Adding a user to a group is how you grant the user access to the data in a domain or a feature of the EOC system. You could even set up one set of groups that only grant access to features and another set that grant access to data.

However you decide to organize your users and groups, you should design a plan before installation while designing your domains and stick with it.

3.4 Privileges

The EOC system defines two different sets of privileges, Feature Privileges and Domain Privileges. As the name implies, Feature Privileges grant group members the ability to use a specific feature in the EOC. Table B lists the Feature Privileges defined by the EOC system.

Table B —Feature Privileges

Data Mining | Convoy Search
Data Mining | Cross Search
Data Mining | Reads/Alarms
Lists | List Names
Lists | List Plates
User Config | Group Manager
User Config | My Profile
User Config | User Manager
System | Audit Messages
System | Device Manager
System | Log Messages
System | System Tasks
System | App Settings
Monitoring Tools | Dashboard
Monitoring Tools | Dispatcher

Domain Privileges grant group members the ability to view or edit specific types of data or perform system administration tasks on data within a domain. Table C lists the Domain Privileges the EOC defines.

Table C — Data Access Roles

DOMAIN PRIVILEGE	COMMENTS
Lists | View	User can view the lists and list entries in the domain.
Lists | Modify	User can modify (create / edit / delete) lists and list entries in the domain.
Reads | Search -- Basic	User can view reads in the domain.
Reads | Modify	User can modify (edit only) reads in the domain.
Reads | Search – Convoy	Reads in the domain can be included in the results of Convoy Searches performed by the user.
Reads | Search – Cross	Reads in the domain can be included in the results of Cross Searches performed by the user.
Reads | Statistics	Reads in the domain can be included in the results displayed by the Dashboard for the user.
Reads | Alarm Validation	User can mark alarms in the domain Correct or Incorrect.
Saved Search | Modify	User can modify (create / edit / delete) saved searches in the domain.
Saved Search | View	User can view saved searches in the domain.
System Config | Modify	User can modify (create / edit / delete) sites in the domain and can perform system admin tasks in CarSystem for sites that belong to the domain.
System Config | View	User can view sites in the domain.
Users | Modify	User can modify (create / edit / delete) users that belong to the domain.
Users | View	User can view users in the domain.
User Groups | Modify	User can edit (create / edit / delete) groups in the domain.
User Groups | View	User can view groups in the domain.

As you can see, the EOC defines at least two privileges for each data type, a view privilege and a modify privilege (for Reads, the Reads | Search Basic privilege is the corresponding view privilege). If a user has the privilege to modify a type of data, they also have the privilege to view that type of data. For example, it is not possible to grant the Lists | Modify privilege and not also grant the Lists | View privilege to a group.

The System Config privileges are required to perform the tasks on the System menu. They also allow a user to use CarSystem's advanced configuration options and its Parking Lot Selector. See the *CarSystem Users' Guide* for more information.

3.5 Search Related Privileges

The Reads | Search - Convoy, Reads | Search – Cross, and Reads | Search – Statistics privileges are used to limit the data that is returned for a user of the Convoy Search, Cross Search, and Dashboard

features, respectively. They help limit the information a user can extract from the database and may be useful to meet data accessibility requirements imposed due to local statutes.

Consider three users, an administrator, a detective working a narcotics investigation and a uniformed officer who drives a beat:

- There's no reason why the uniformed officer would need to perform Convoy or Cross Searches, or use the Dashboard's reports, so that user should not have any of these privileges.
- The detective can make good use of the Convoy and Cross Search features to investigate drug shipments, so they should have the corresponding privileges. They really don't need the Reads | Statistics privilege, though, as they are not interested in monitoring data backlogs, so they should not have that privilege.
- The administrator needs the Reads | Statistics privilege because they do care about data backlogs. They do not need to perform Convoy or Cross Searches, however, so they should not have those privileges.

Even though the detective may perform Convoy & Cross Searches, they may not need to do so with all data in all domains. In that case, they should only have the Reads | Search – Convoy & Reads | Search – Cross privileges in the required domains. Doing so will prevent them from seeing data they are not permitted to see.

3.5.1 Alarm Access Rules

For most data types, a user must have the corresponding view privilege to be able to see that type of data and must have the modify privilege to be able to make changes. The exception is alarm data.

Alarms are created when a read's plate matches an entry in a List, or when a read's plate does not match an entry in a White List. When it is created, the alarm is added to the domain that the list entry belongs to. This is necessary to prevent users who don't have access to the list from discovering that it exists.

In order for a user to be able to view an alarm, they must be able to see both the read and the list entry that the alarm was generated from. The user therefore has to have the Reads | Search -- Basic permission in the domain that the read belongs to and the Lists | View privilege in the domain that the list entry belongs to.

To be able to mark the alarm correct or incorrect, the user must be able to see the alarm and must have the Reads | Alarm Validation privilege in the domain that the alarm belongs to. If a user can see an alarm but they do not have Reads | Alarm Validation in the correct domain, they will not be able to change it.

Lastly, to be able to add Officer Notes to an alarm, a user has to have the List | Modify privilege in the domain that the alarm belongs to.

To help make this clear, consider the following example.

> An officer is operating a vehicle equipped with LPR cameras and the CarSystem software. This vehicle is represented in the EOC as the site named 1A12 in the Mobiles domain.
>
> Unknown to the officer, there is a covert investigation under way which has created a list in the Special Investigation 27 domain. The officer's user account does not have the List | View privilege in the Special Investigation 27 domain.
>
> As the officer is driving, she passes a vehicle whose license plate is on the Special Investigation 27 list. The license plate is read and processed by CarSystem. A read is generated, and the read belongs to the Mobiles domain, since the car site 1A12 is in the Mobiles domain. The officer has rights to see reads in the mobiles domain, so it is displayed to her.

An alarm is also generated, since the plate matches the entry for it in the Special Investigation 27 list. Even though the officer can see the read, she can't see the alarm, since she can't see the list. The alarm is never displayed to her in the car.

Back at headquarters, a detective who is a member of the team conducting the investigation has the Reads | Search – Basic privilege in the Mobiles domain and has the List | View privilege in the Special Investigation 27 domain. He is running the Dispatcher feature of the EOC system. When the EOC receives the alarm from the car 1A12, the alarm is displayed to him. If the detective also has the Reads | Alarm Validation privilege in the Special Investigation 27 domain, he will be able to mark the alarm correct. If he has Lists | Modify privilege in the Special Investigation 27 domain, he will also be able to add Officer Notes to the alarm.

3.5.2 Privileges from Multiple Groups

If a user belongs to more than one group, the privileges that user has are cumulative across all of the groups. That is, the privileges the user has are the sum of all of the unique privileges granted by all of the groups. Let's consider the following example to make this easier to understand.

There is a user who belongs to two groups, CarSystem and Special Investigation 27. The CarSystem group grants its members the Lists | View privilege in the Local Hotlists domain, but not the Lists | Modify privilege. The Special Investigation 27 group, on the other hand, does grant its members Lists | Modify privilege in the Local Hotlists domain. When this user logs in to CarSystem or the EOC, they have both the Lists | View and Lists| Modify privilege in the Local Hotlists domain.

If the Special Investigation 27 group also has the Lists | View privilege in the Covert Ops domain, but the CarSystem group does not, the user will also have Lists | View privilege in the Covert Ops domain. Users who are members of the CarSystem group but are not members of the Special Investigation 27 group, on the other hand, will not have the Lists | View privilege in the Covert Ops domain.

3.6 Installed Domains, Groups and Users

The first time it is run, the EOC installation process creates the following domains:

Table D —Domains Created by Installer

DOMAIN	PURPOSE
Administrative	Contains all data related to system administration
Covert Ops	Contains data related to covert investigations
Fixed Sites	Contains data related to fixed CarSystem installations
Local Hotlists	Contains all internal lists
Mobiles	Contains data related to all mobile CarSystem installations
NCIC Hotlist	Contains the NCIC List.

The installation process creates the following groups:

Table E — Groups Created by Installer

GROUP	PURPOSE
Administrators	Grants full administration privileges to its members in all installed domains
CarSystem	Grants required privileges to all CarSystem operators
Patrol	Grants required privileges to patrol officers
Traffic	Grants required privileges to traffic officers
Investigations	Grants required privileges to detectives

Finally, the installation process creates the following users:

Table F — Users Created by Installer

USER	PURPOSE
Administrator	Default administrator
CarSystem	Default CarSystem user

These defaults give you the necessary tools to begin configuring your system.

The Administrator group initially has full privileges in all domains created by the installer. By default, the CarSystem group is granted the following privileges:

Table G — Installed CarSystem Group Privileges

DOMAIN	PRIVILEGES
Fixed Sites	Lists | View
Local Hotlists	Lists | View Lists | Modify
Mobiles	Reads | Alarm Validation Reads | Search – Basic Reads | Search – Convoy Reads | Search – Cross Reads | Statistics

Note that the CarSystem user is intended to be used to log into CarSystem in installations which do not require the user to log in as themselves. The CarSystem user is the only member of the CarSystem group after installation. If you require users to log in as themselves when logging into CarSystem, then you need to create a unique user ID for each CarSystem user and add them to the CarSystem group, or another group of your choosing.

If you need to, you can change the privileges assigned to the CarSystem group at any time.

3.7 Supporting Covert Operations

There may be instances where a covert investigation is ongoing and it is desired to track the movements of one or more known vehicles. In addition, normal EOC & CarSystem operators should have no knowledge of the investigation or of the vehicles being surveilled.

The EOC system supports this use case using the following configuration.

(1) Decide which domain to use for the investigation. You may either use the default Covert Ops domain created by the installer or create a new one for the specific investigation. See *Creating a Domain* on page 44 for details. If you do create a new domain, we recommend you use the name of the investigation as the name of the domain.

(2) Create a new group that all members of the covert operation team must belong to. See *Create a Group Procedure* on page 30 for instructions. We recommend you use the name of the investigation as the name of the group. Add the group to the domain for the investigation you decided to use in step (1). Be sure to grant the group the proper privileges in the domain:

- Grant the Lists | View privilege to the group so group members can see any lists in the domain.
- Grant the Lists | Modify privilege so the team can manage their own lists.
- Grant the Reads | Alarm Validation privilege so the team can mark any alarms that are generated against their lists as correct or incorrect.
- It is important that no other group has these privileges in the covert operation's domain to ensure confidentiality.

(3) Add the users for the investigation's team members to the group you created in step (2). It is important that only members of the investigation team or anyone the team wishes be granted access are added to this group!

(4) An administrator or one of the group's members now creates one or more lists for the investigation. The lists can be named anything desired, but including the investigation's name in the group's name would make administering everything easier. Make sure the list belongs to the domain you decided to use in step (1).

(5) An administrator or the one of the group's members can add the plates of interest to the list or lists created in step (4).

Once all of these steps are completed, any reads that are captured for any vehicles in the investigation's lists cause alarms to be generated, no matter what domain the reader belongs to. Since the list belongs to a different domain, and only team members can see the list and its contents, only the team members will be able to see the alarm and will know that the plate is under surveillance. Even the operator of the CarSystem which captured the read will not know that the alarm was created if he is not a member of the investigation's group.

The EOC provides two mechanisms that can be used by the team to be notified when alarms on their lists are generated:

- They can run Dispatcher and can set it up to only display alarms generated from the investigation's lists.
- Each team member can modify their user profile to have notification emails sent to them when alarms are generated from the list.

Either notification method will work, though Dispatcher would require the user to be logged into the EOC, while the email notification would not. The team members can even use both mechanisms at the same time.

4 User Configuration

4.1 Introduction

The EOC can run in one of two different user authentication modes: **SQL Server Mode** and **Active Directory Mode**. Please see *EOC User Authentication Modes* on page 11 for more details. This chapter describes how to manage users and groups in either authentication mode.

4.2 Managing Users — SQL Server Mode

To create a User perform the following steps:

(1) Select **User Config > User Manager** from the menu bar across the top of the main screen.

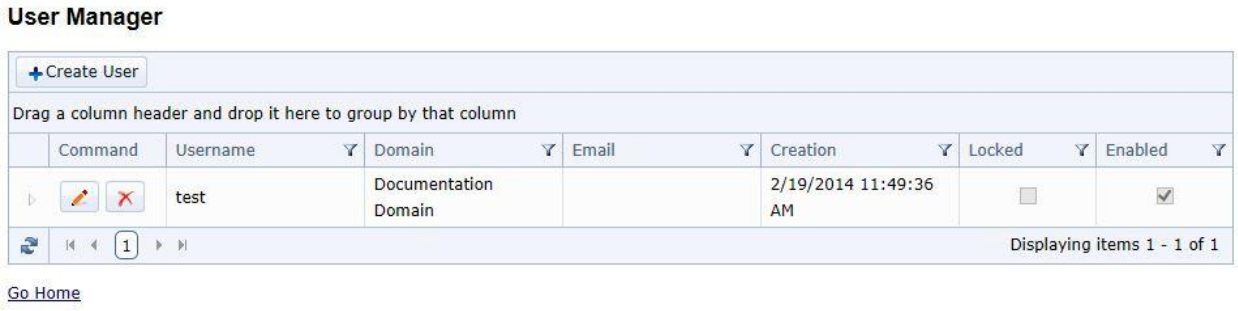

Figure 1 — User Manager Screen

(2) Press the "+ Create User" button and the screen shown in Figure 2 will appear.

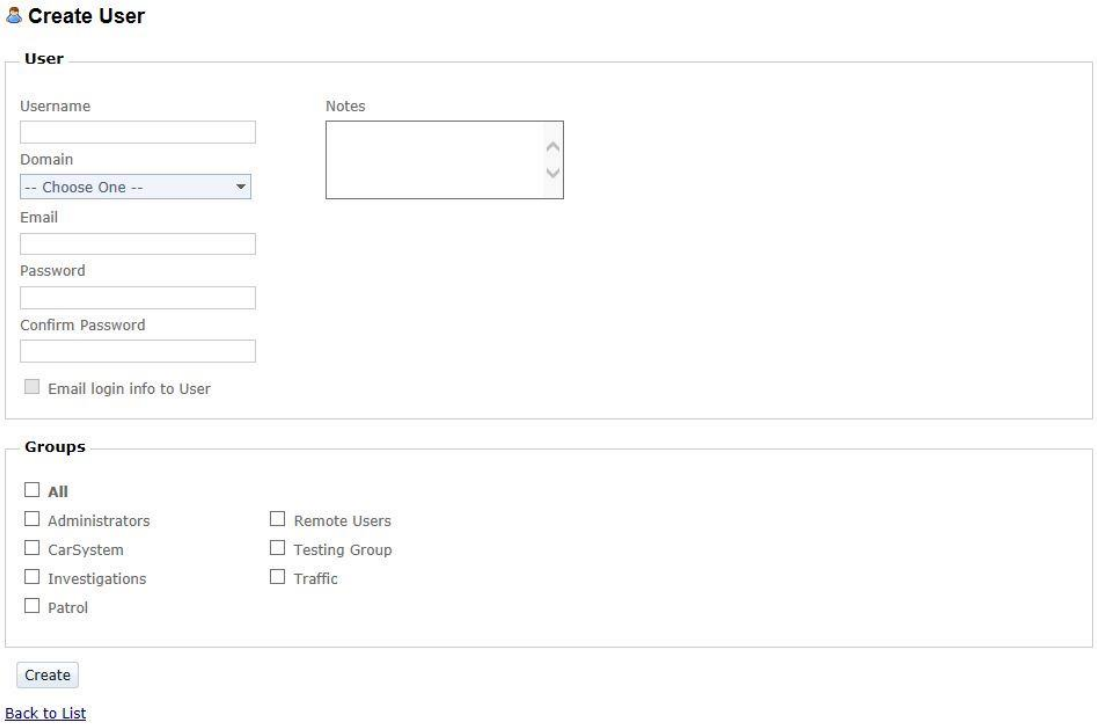

Figure 2 — SQL Server Mode Create User Initial Screen

(3) Type in the **Username** for the new user.

(4) Select the EOC **Domain** in which you want to create this user. You will only see domains to which you have access.

(5) Enter an optional **Email Address** associated with the user.

(6) Add a **Password** and then confirm the password by typing it in again.

(7) The optional **Notes** box can be used to spell out a user's name or provide any notes needed.

(8) Select the checkbox to email the login information to the new user. (The message will also contain the URL to the EOC implementation.)

(9) Select the groups to which the new user will belong by checking the boxes.

(10) Press **Create** to create the new user.

4.2.1 View a User's Details

You can view a user account's details, including the following attributes:

- Username
- Domain
- Email Address
- Creation date and time, and
- Whether the user is Enabled or Locked.

To view a user's details, select **User Config > User Manager** from the menu bar across the top of the main screen and the screen shown below in Figure 3 will appear. This allows you to view a list of all users. Clicking on the triangle will display the Groups the user is assigned to.

Figure 3 — SQL Server Mode User Details Screen

4.2.2 Edit a User's Details, including Password

To edit a user's details, perform the following steps:

(1) Select **User Config > User Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 4.

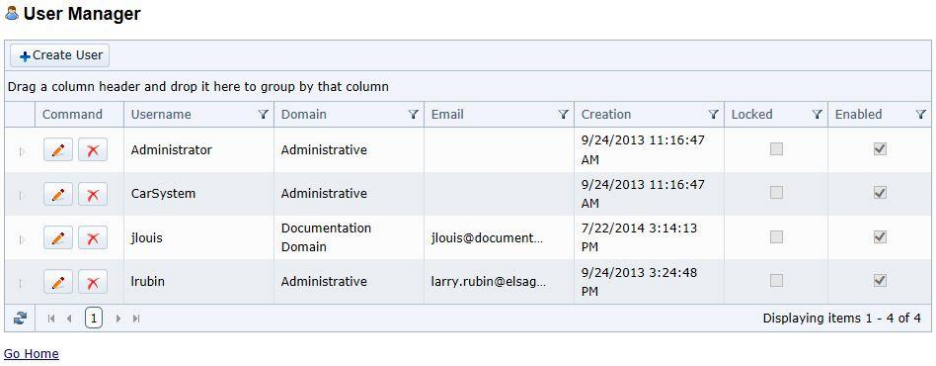

Figure 4 — SQL Server Mode User Details Screen

(2) Press the **Edit** Icon (pencil) next to the user whose attributes you want to edit and a screen similar to the one shown in Figure 5 will appear. Note that the Password fields will be blank.

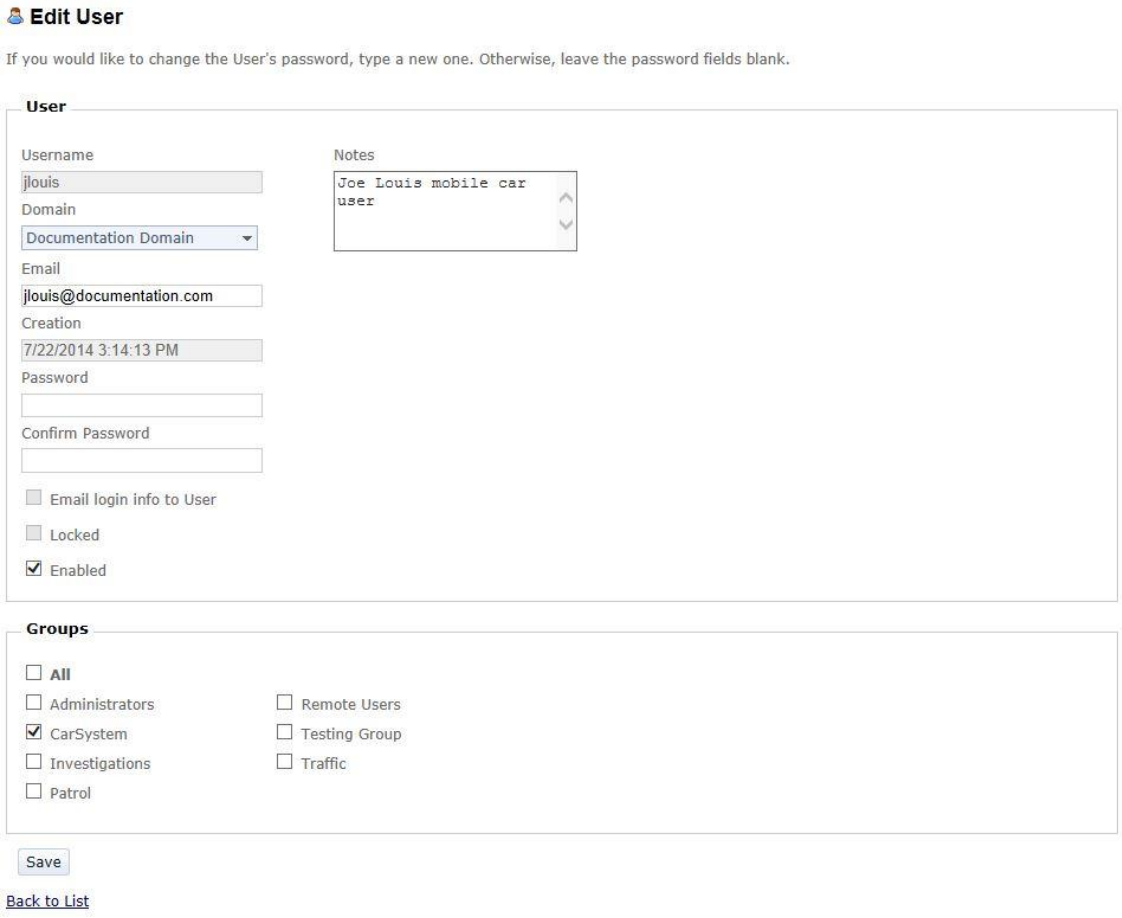

Figure 5 — SQL Server Mode Edit User Screen

(3) Edit the fields you need to edit. If you wish to change the user's password you must enter the new password and re-enter it in the Confirm Password field. Leaving these fields blank will leave the user's password unchanged.

(4) Press the **Save** button to save the changes.

4.2.3 Delete a User

To delete a user, perform the following steps:

(1) Select **User Config > User Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 6.

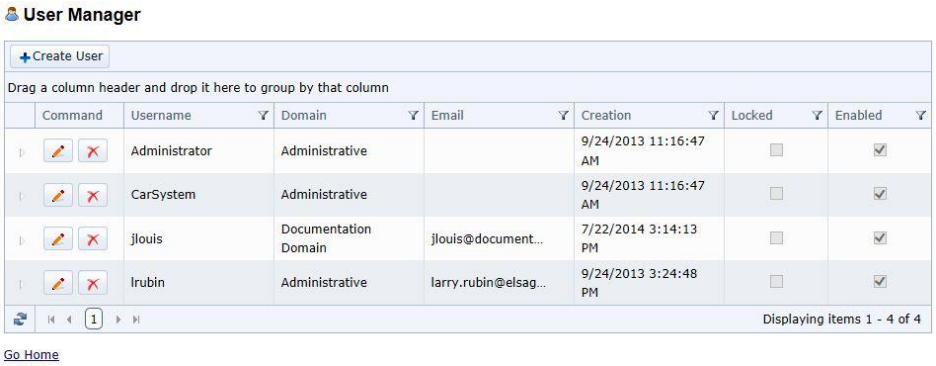

Figure 6 — SQL Server Mode User Details Screen

(2) Press the **Delete Icon** (red X) next to the user you want to delete and you will see the prompt shown in Figure 7.

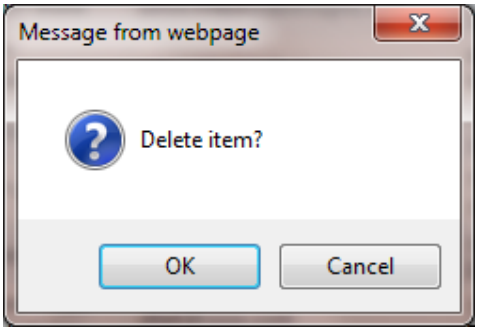

Figure 7 — SQL Server Mode Delete User Confirmation

(3) If you press **Cancel**, the user account will not be deleted.

(4) Press **OK**. The user account is deleted.

4.2.4 Exporting the User List

The User List can be exported to a standard CSV (Comma Separated Values) file. Follow these steps to export the User List.

(1) Select **User Config > User Manager** from the menu. You will see a display of all the EOC's current users for which you have View or View/Modify permissions.

(2) Click **Export**. The screen shown in Figure 8 is as it would appear if you are using Microsoft Internet Explorer.

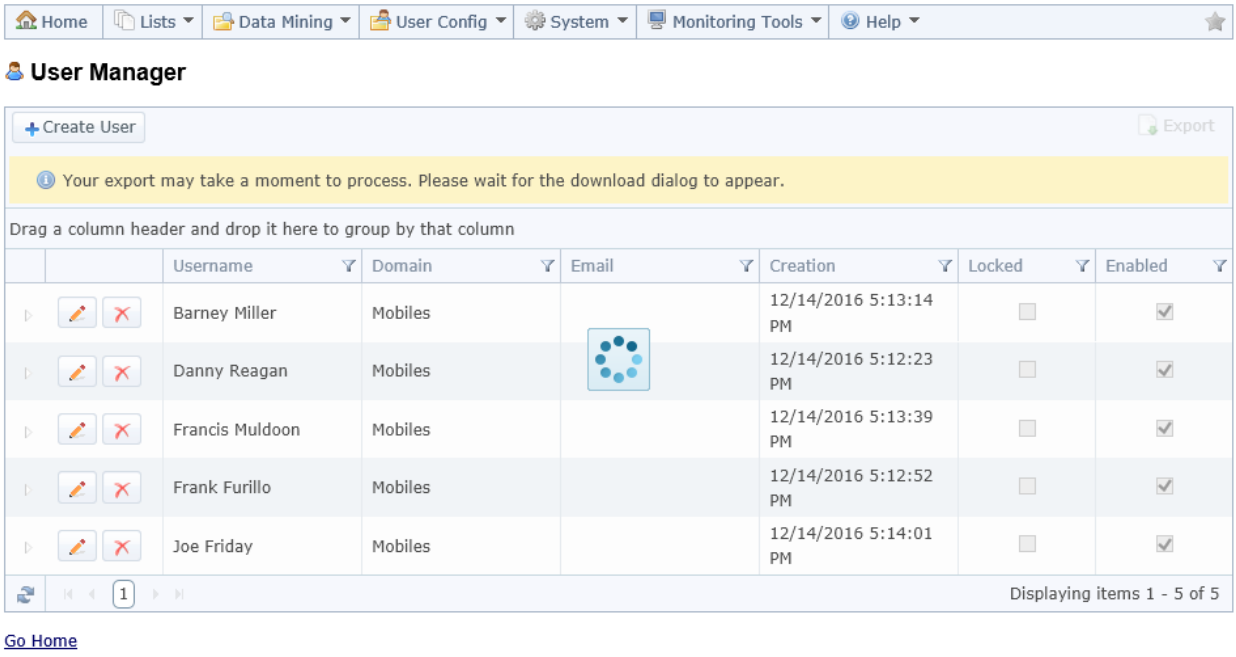

Figure 8 — Export User List in Progress

(3) When the export is complete, you will see a save dialog as shown in Figure 9. Select **Save** and the file will be saved to your Downloads folder (in Windows 7).

NOTE: The prompt shown is the one generated by Internet Explorer. The prompt will look different if you use a different browser, like Firefox, Chrome, or even a different version of Internet Explorer.

Figure 9 — Save Exported User File

4.3 Managing Users — Active Directory Mode

Managing users in Active Directory Mode is slightly different from managing them in SQL Server Mode because authentication in Active Directory Mode is handled by Windows Active Directory.

NOTE: When you create a user in EOC, you are associating an existing Windows username and password with an EOC user account. Therefore, when you manage users in EOC in Active Directory Mode, any changes you make to an EOC user **will not be reflected** in the Windows user account. Likewise if you delete a user, the user will only be deleted inside the EOC, not in Windows. Deleting a user account removes that user's access to the EOC only.

4.3.1 Create a User

NOTE: If a user does not already exist in Windows Active Directory, you will not be able to create an EOC user; create the Windows Active Directory user account first.

(1) Select **User Config > User Manager** from the menu. You will see a display of all the EOC's current users. Note that the display will remind you that you are running in Active Directory Mode.

(2) Press the "+ Create User" button and the screen shown in Figure 10 will appear.

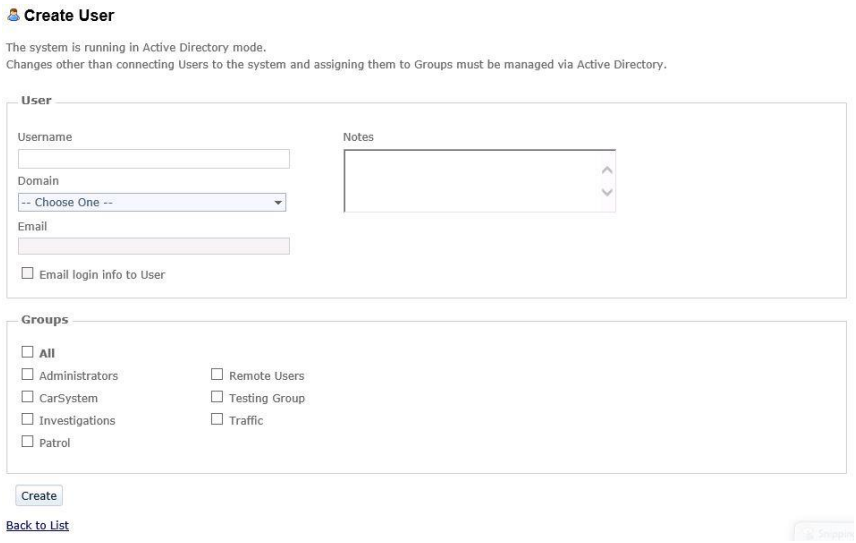

Figure 10 — Active Directory Mode Create User Initial Screen

(3) Type in a **Username** for the new user. The username must be in the same format as the Windows Active Directory username, for example, **joe.louis**. As you type characters in, the EOC system will display possibilities that you can select.

NOTE: There is no place to set a password, since Active Directory Mode uses Windows authentication to control access to EOC. The EOC user's password will be the same as the password to the Window user account. The **Email Address** will automatically fill in once you enter the existing Windows user.

(4) Select the EOC **Domain** in which you want to create this user. You will only see domains to which you have access.

(5) Select the checkbox to email the login information to the new user. (The message will also contain the URL to the EOC implementation.)

(6) The optional **Notes** box can be used to spell out a user's name or provide any notes needed.

(7) Select the groups to which the new user will belong by checking the boxes.

(8) Press **Create** to create the new user.

4.3.2 View or Edit a User's Details

You use the same procedure to view a user's details or to edit a user's details regardless of the current authentication mode. Use the steps that follow:

(1) Select **User Config > User Manager** from the menu. You will see a display of all the EOC's current users. Note that the display will remind you that you are running in Active Directory Mode.

(2) Press the **Edit** button next to the user whose attributes you want to view or edit and a screen similar to the one shown in Figure 11 will appear.

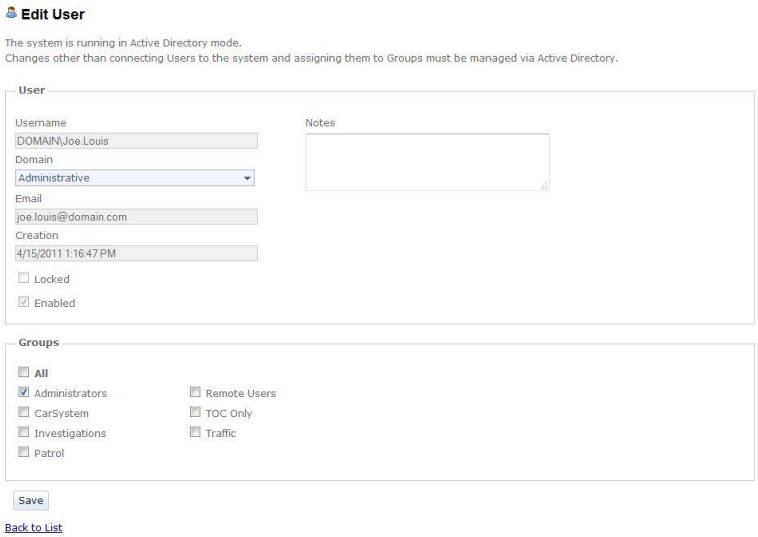

Figure 11 — Active Directory Mode View/Edit User Screen

(3) Non-editable fields will be grayed out. Edit fields that you want to change.

(4) Press the **Save** button to save the changes.

4.3.3 Delete a User

To delete a user perform the following steps:

(1) Select **User Config > User Manager** from the menu. You will see a display of all the EOC's current users. Note that the display will remind you that you are running in Active Directory Mode.

(2) Press the **Delete Icon** (red X) next to the user whose attributes you want to view or edit. You will see the screen shown in Figure 12.

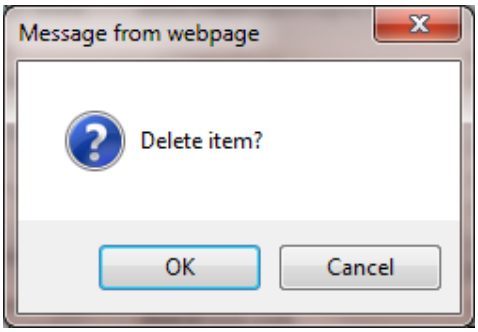

Figure 12 — Active Directory Mode Delete User Confirmation

(3) Press **OK**. The EOC user account is deleted and the user can no longer log into the EOC. The windows active directory user account is unaffected.

4.3.4 Exporting the User List

The process for exporting the user list is the same for both Active Directory and SQL modes. See *Exporting the User List* on page 27 for details.

4.4 Managing Groups

Creating and managing groups operates exactly the same in SQL Server Mode and Active Directory Mode.

4.4.1 Create a Group Procedure

To create a group, perform the following steps:

(1) Select **User Config > Group Manager** from the menu bar across the top of the main screen.

(2) Press the "+ Create Group" button and the screen shown in Figure 13 will appear.

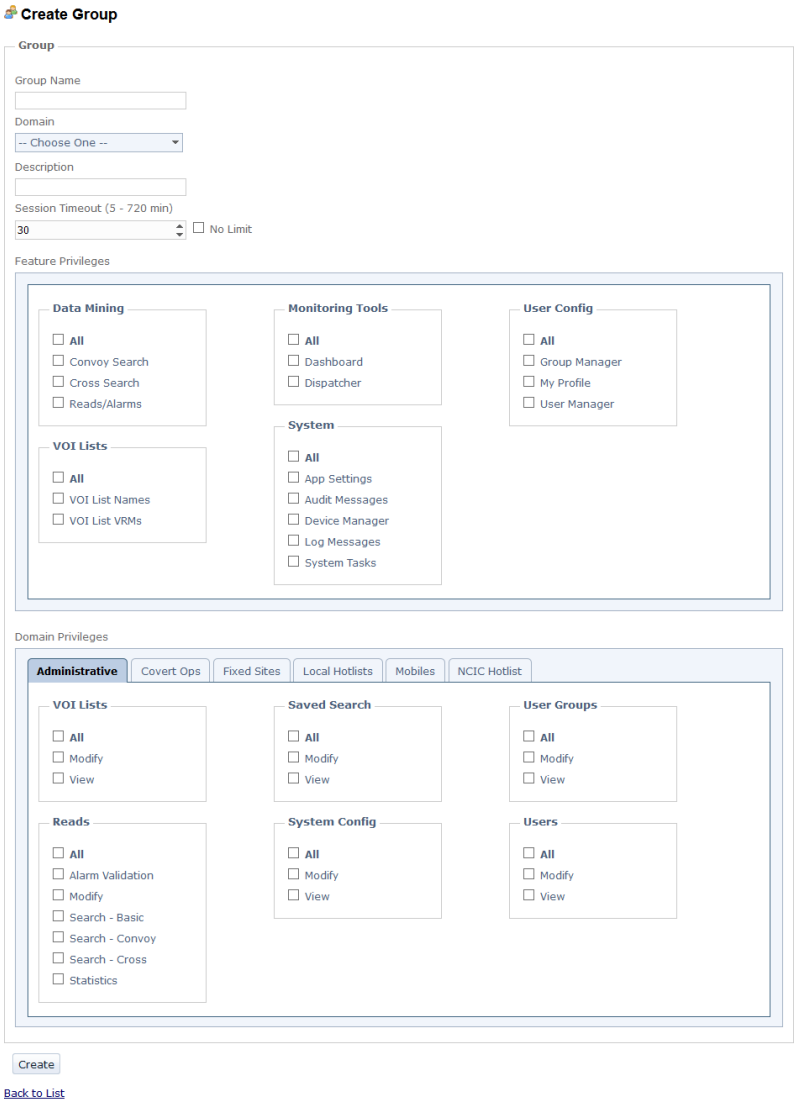

Figure 13 — Create Group Initial Screen

(3) Type in the Group Name for the new group.

(4) Select the EOC **Domain** in which you want to create this group from the **Domain** dropdown. You will only see domains to which you have access. (The named domain tabs across the bottom allow you to specify the permissions that members of this group will have in each of those domains.)

(5) Enter a **Description** for the group.

(6) Add a **Session Timeout** in minutes. This controls how long a session initiated by someone in this group will stay active if there is no activity. Check **No Limit** to allow users to stay connected indefinitely.

(7) Select the checkboxes to assign the EOC Feature Privileges for this group.

(8) Select the checkboxes to assign individual Domain Privileges for this group.

(9) Press **Create** to create the new group.

4.4.2 View a Group's Details

You can view a group's details, including the following attributes:

- Group Name
- Domain — Domain the group belongs to
- Description — Group's description, and
- Session Timeout — How long a session will stay active if there is no activity.

To see a group's details, select **User Config > Group Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 14. This allows you to view a list of all groups. Clicking on the triangle will display all Users assigned to the Group.

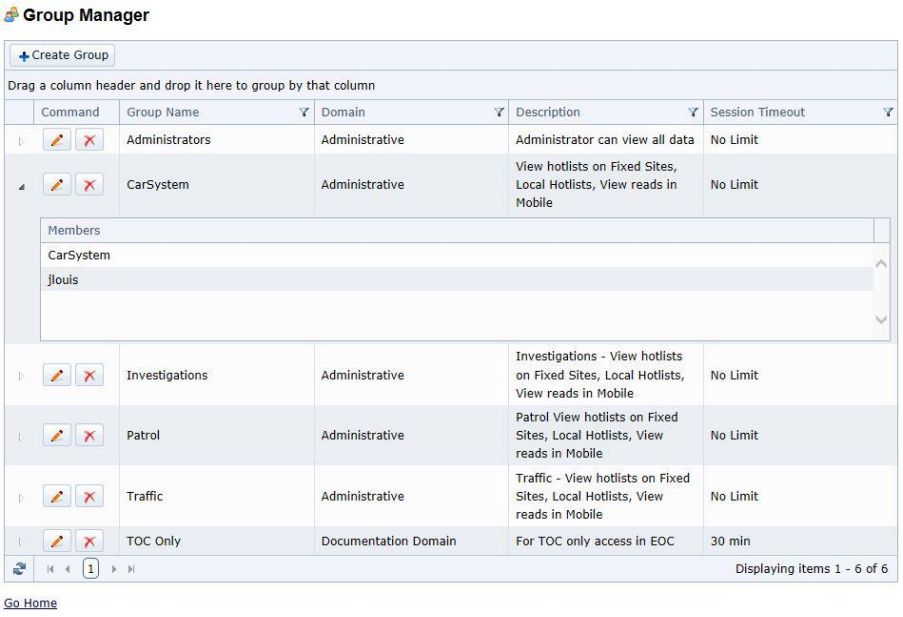

Figure 14 — Group Details Screen Showing Members

4.4.3 Edit a Group

To edit a group perform the following steps:

(1) Select **User Config > Group Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 15. Press the **Edit Icon** (pencil) next to the group whose attributes you want to edit.

Figure 15 — Group Details Screen

(2) Referring to Figure 16, the **Edit Group** screen is displayed.

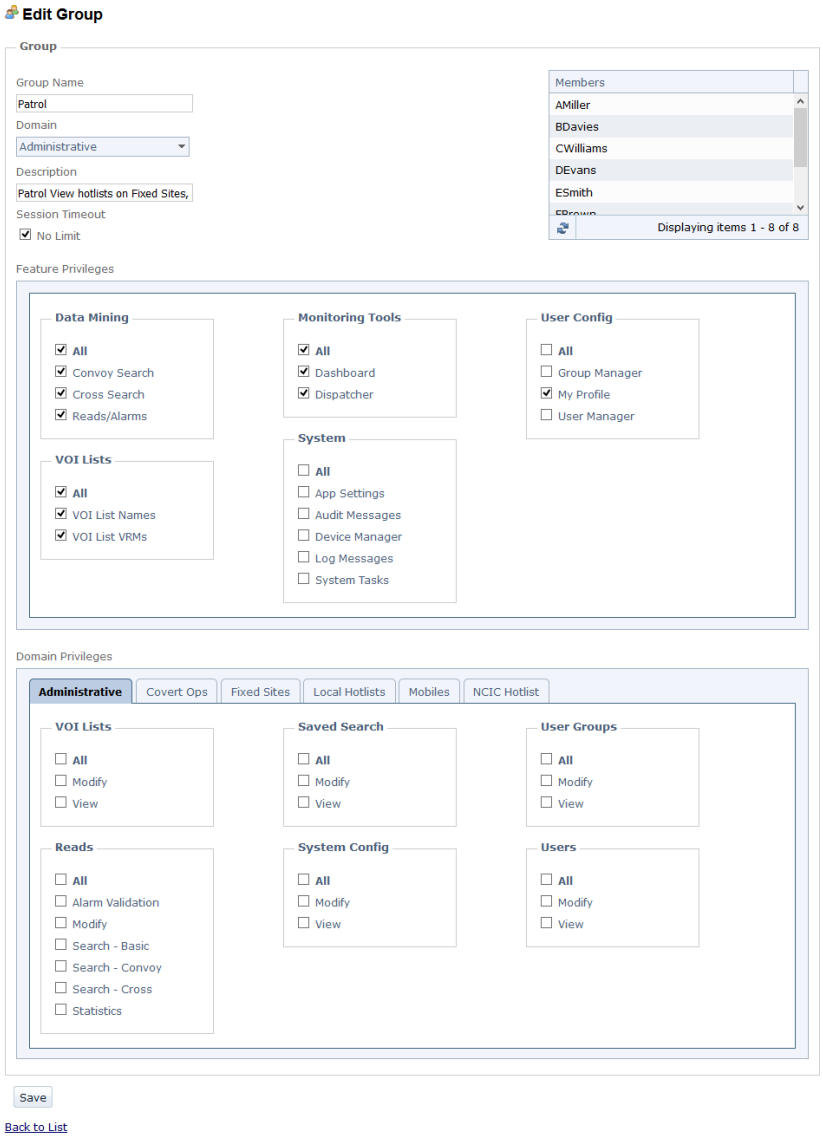

Figure 16 — Edit Group Screen

(3) Edit the fields and/or privileges you need to edit.

(4) Press the **Save** button to save the changes.

4.4.4 Delete a Group

To delete a group perform the following steps:

(1) Select **User Config > Group Manager** from the menu bar across the top of the main screen. You will see the screen shown in Figure 17.

Figure 17 — Group Details Screen

(2) Press the **Delete Icon** (red X) next to the user whose attributes you want to edit and you will see the screen shown in Figure 18.

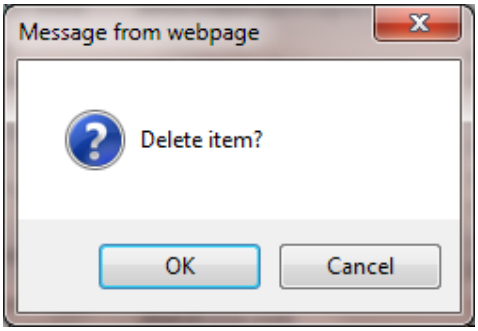

Figure 18 — Delete Group Confirmation

(3) Press **Cancel** to keep the group from being deleted.

(4) Press **OK**. The group is deleted from the system.

4.5 Group Manager Privileges Examples

The Documentation Group has the permissions shown below in Figure 19.

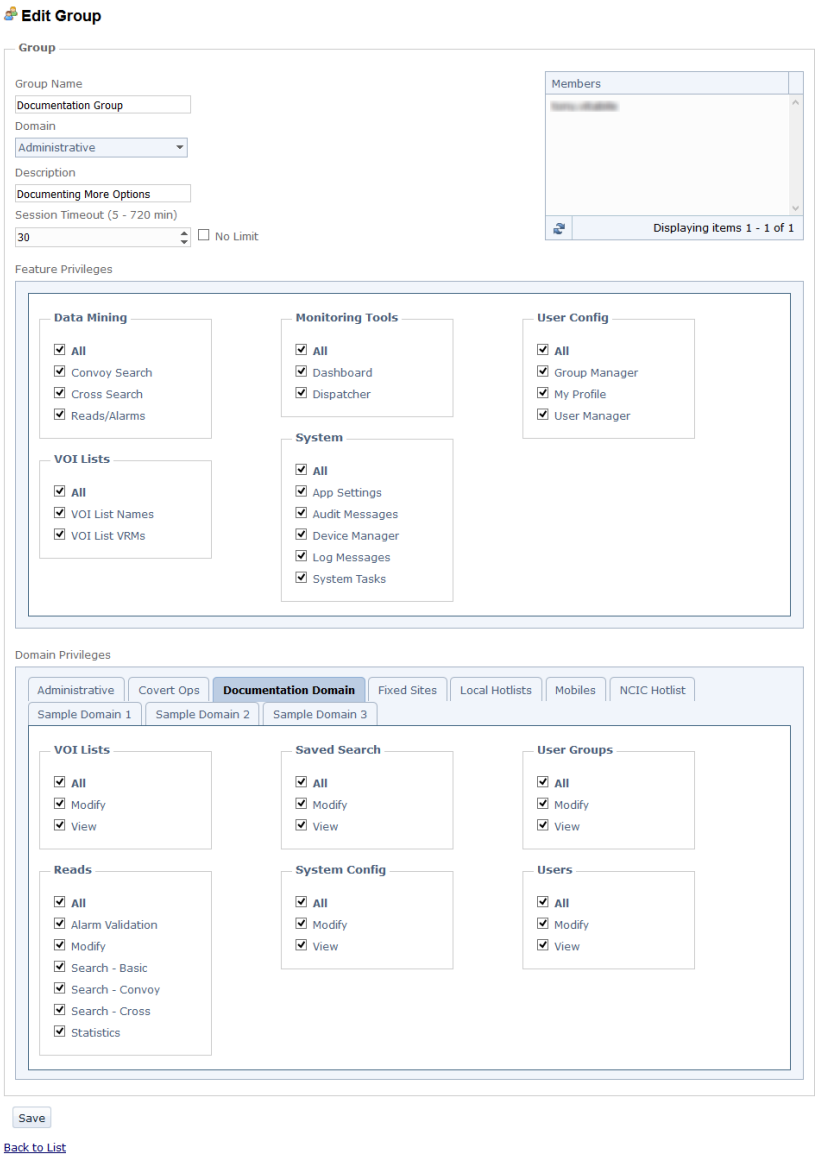

Figure 19 — Group Permissions Set

Referring to Figure 19, notice that the group **Documentation** has full access to all areas of the EOC based on the **Feature Privileges** selected and for the selected **Documentation** Domain.

In this case, a user account that is only a member of the **Documentation** group can view, search or modify list data, see read data in all search features, create and view other users, perform system configuration tasks, as well as view, create and edit user groups. All these permissions apply to the **Documentation** domain only (the selected tab under Domain Privileges). You can also see a list of the group's members in the upper right.

NOTE: Referring to Figure 20, in a different domain, say **Administrative**, the **Documentation** group has no Domain Privileges at all. This means that a user account associated only with the **Documentation** group cannot view read data from any devices associated with the **Administrative** domain. In fact, a user account only associated with the **Documentation** group will not even see the **Administrative** domain when they log into the EOC.

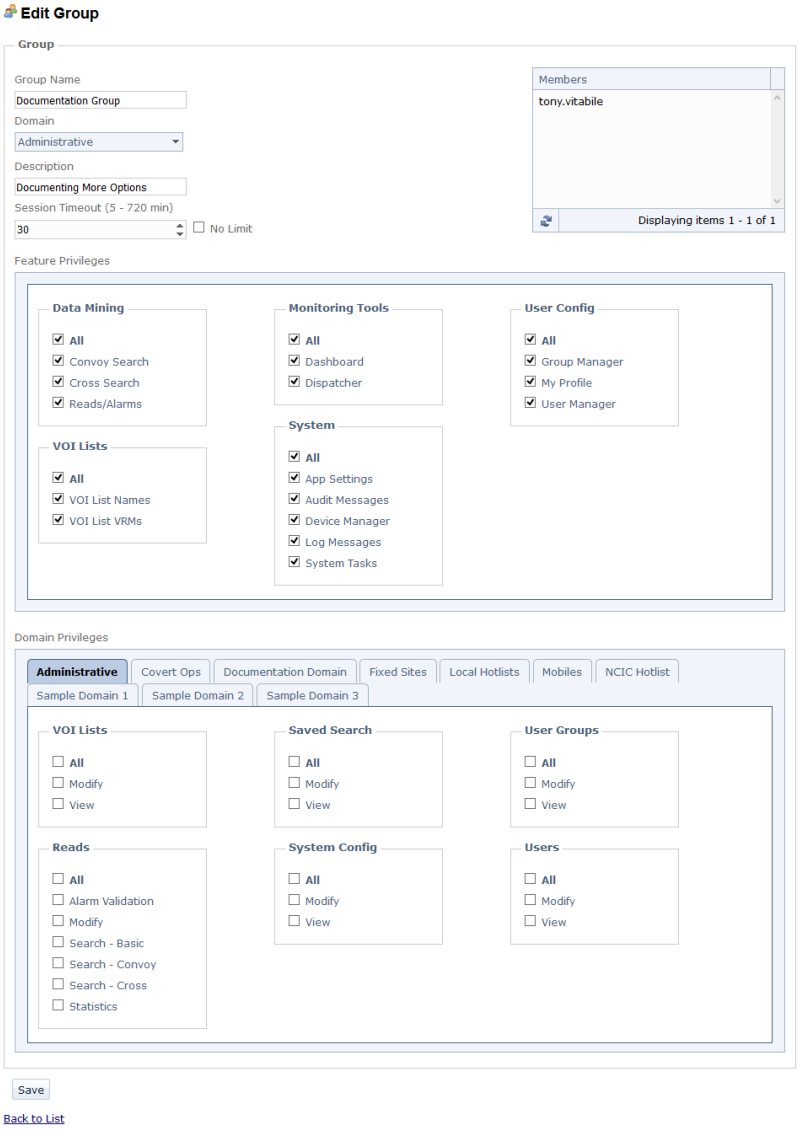

Figure 20 — Group Permissions Not Set

NOTE: Referring to Figure 21 below, the **Dispatcher Only** group only has EOC **Feature Privileges** to **Dispatcher** for the domain **Brewster Lot** (all other domains have no enabled privileges). This means that a user account associated with the **Dispatcher Only** group only has access to the EOC for running Dispatcher and can only see alarm data from **Brewster Lot**. In fact, a user account associated with the **Dispatcher Only** group will not even see any of the other EOC Menu options or domains when it logs into the EOC.

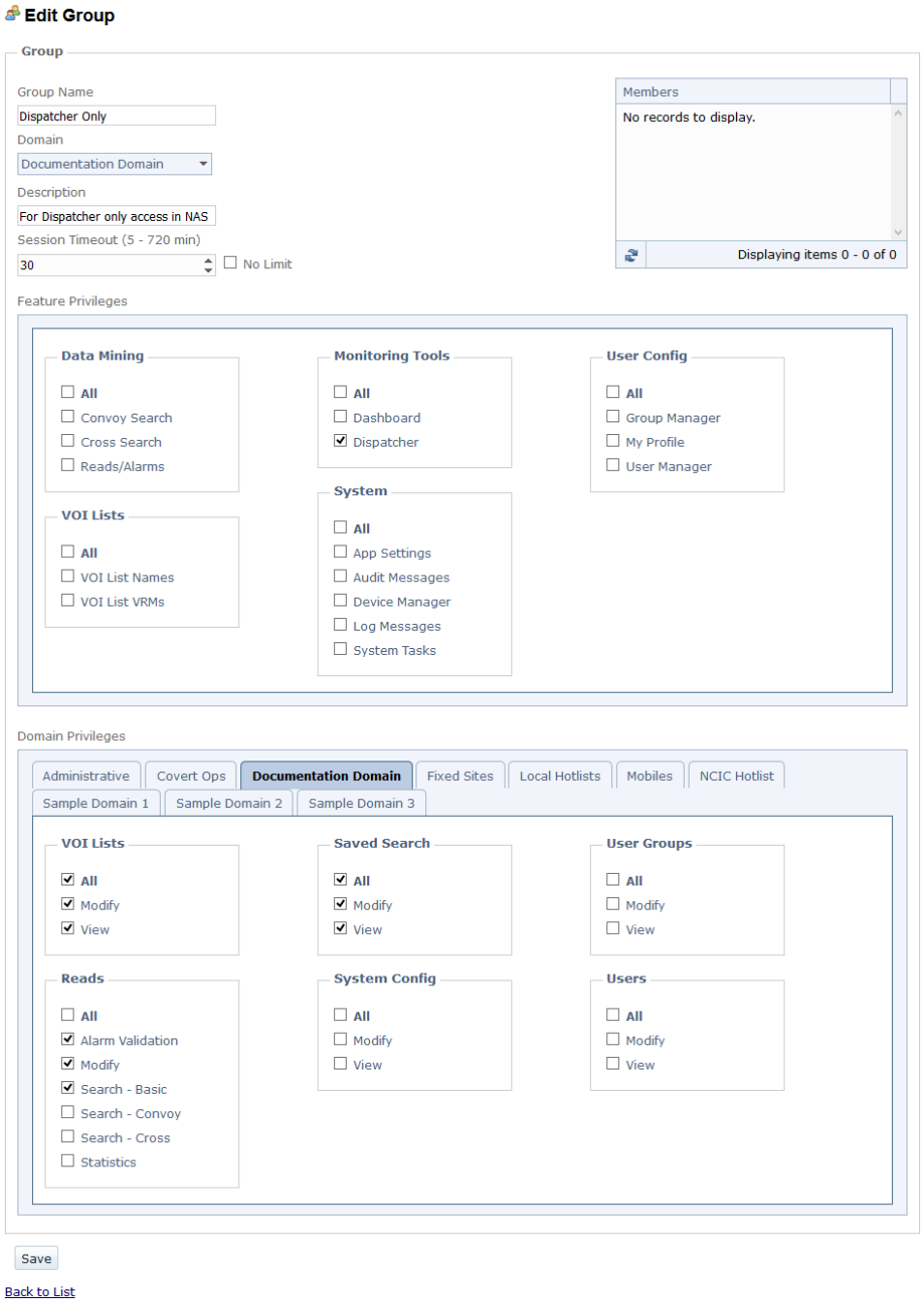

Figure 21 — Group Permissions Feature Restricted

Referring to Figure 22, this is an example of what a **Dispatcher Only** group user would see when logged into EOC. The user only has access under **User Config** to change their password and under **Monitoring Tools** access to **Dispatcher**.

Figure 22 — Group Permissions Dispatcher Only Example

4.6 Create a Profile

The EOC allows you to create a per-user profile that controls various aspects of how that user interacts with the system. The profile controls whether a user receives an email when an alarm sounds against a list or lists or when a System Task of interest has failed. To create a profile, refer to Figure 23 and perform the steps that follow:

(1) To create a profile, log in as the user you want to receive emails.

(2) Select **User Config > My Profile** from the main menu.

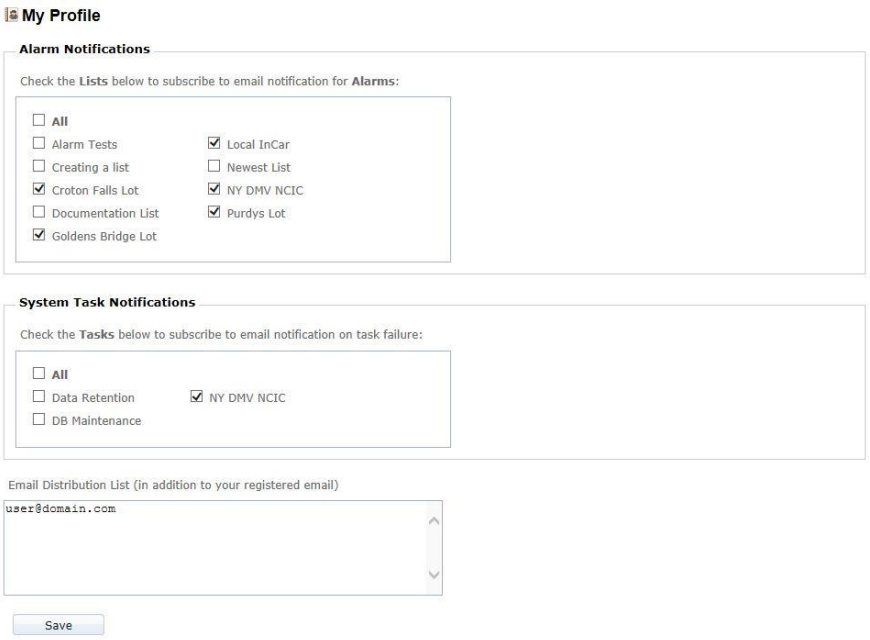

Figure 23 — My Profile Screen

(3) Select the list or lists you want to receive email notifications for when an alarm is generated.

(4) Select the System Task or tasks you want to receive email notifications for when a task fails to complete successfully.

(5) Press **Save**.

NOTE: Email Distribution List allows for duplicate emails to be sent to other email addresses or email distribution lists. This allows an email alert to be sent to someone who does not have access to the EOC. Use a comma to separate email addresses.

5 System Configuration

5.1 Introduction

The **System** tab of the EOC allows you to:

- Set up and manage the organization of your EOC implementation (**Device Manager**),
- Define and schedule system maintenance tasks (**System Tasks**),
- Audit activities within your EOC implementation (**Log Messages** or **Audit Messages**), and
- Modify EOC Application settings (**App Settings**).

5.2 Device Manager

The Device Manager area of the System Configuration tab allows you to set up your local organizations inside EOC, including such elements as:

- Geographical areas
- Organizational groupings
- Vehicles
- Mobile Cameras
- Fixed Cameras, and
- FCUs (Field Control Units).

It is a useful exercise to plot out your site configuration before you start to build it in EOC, although it is simple to reorganize within the EOC. We have included a simple tutorial on how to set up a system below.

Device Manager also allows you to move cameras and other elements easily within EOC, as well as enable and disable individual elements.

5.2.1 Types of Nodes

Device Manager allows for five different types of elements or **nodes**:

- Camera — Represents an LPR attached to a Car or FCU.
- Car — A container for mobile cameras.
- FCU (Field Control Unit) — A container for fixed cameras.
- Folder — A grouping of nodes, representing domains, geographical areas and/or organizational groups, and
- Server — A remote program or service that interfaces with, or is a component of, the EOC.

Each Car or FCU runs one instance of the CarSystem software. Multiple FCUs need multiple instances of CarSystem running. Each CarSystem instance may have any number of cameras connected to it.

For single installations, one Server node represents the EOC. For split installations, there will be a Server node for each Aggregator, Injector, and Web Server that is part of the EOC. These will initially all be named EOC Server, but they should be renamed to the particular EOC component. See *Elsag Plate*

Hunter® EOC Installation Guide for more details about the EOC components. Additionally, there will be a Server node for any remote server that has been set up for Data Sharing.

A node in the tree that has other nodes under it is called a **branch**. You can delete a single node or an entire branch at once. The exception is a domain node. You can delete all of the domain's child nodes, but you cannot ever delete a domain.

5.2.1.1 Sample Hierarchy

A hierarchical diagram of a typical EOC system shows how the different types of nodes relate.

Consider this scenario: You have three towns in your county, each of which has one car with two cameras installed and two fixed cameras at various locations in each town. Your system hierarchy (with the type of node in parentheses) would look like this.

NOTE: Nodes of the same type below the parent level should be given unique names within their domain when you create them. For example, refer to Figure 24 below.

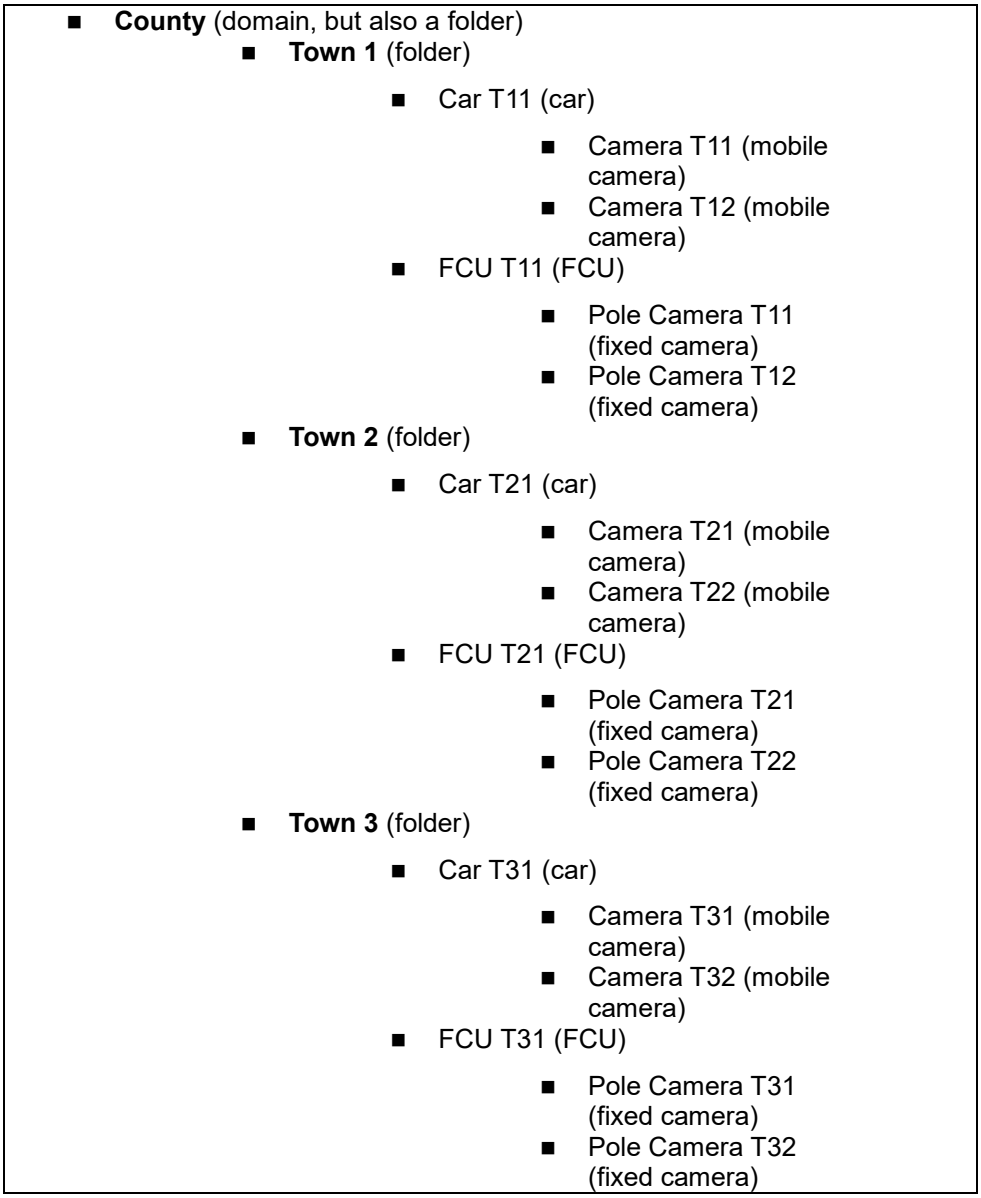

Figure 24 — Sample EOC System Hierarchy

5.2.2 Prerequisites

Before creating the system configuration for your EOC implementation, you must create the domains for it. A domain is how the EOC collects data and sets the permissions for access to it.

The EOC is installed with a number of default domains, as well as default users and groups. See *Getting Started — Domains, Groups, and Users* on page 12 for lists of the domains and groups created by the EOC installer.

5.2.3 Creating a Domain

An EOC domain groups related data and controls permissions to access that data. For example, you could use a separate domain inside the EOC to collect data from a list that you wish to restrict access to. Please see *Chapter 3 - Security System* on page 14 for more information about how domains and privileges function. See *Supporting Covert Operations* on page 20 for an example of how to restrict access to data.

To begin, click on **System Tasks > Device Manager**. The page shown in Figure 25 is displayed.

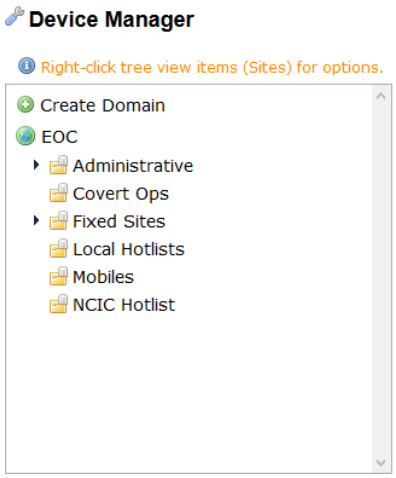

Figure 25 — Device Manager

In the **Device Manager**, you will not see the **Create Domain** function unless you have permissions to create a domain.

NOTE: You cannot delete a domain once you have created it. You can, however, rename one.

To create a domain, perform the following steps:

(1) Press the **Create Domain** button and the screen shown in Figure 26 will appear.

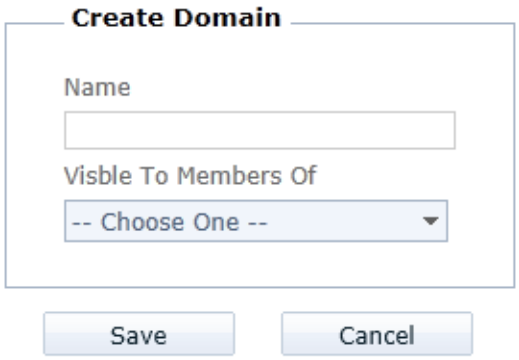

Figure 26 — Create Domain Initial Screen

(2) Select a group whose members will administer the domain. You must be a member of this group to select the group. When the domain is created, the group you select will be granted full administrative privileges to it.

NOTE: The groups listed in the "Visible To Members Of" list are limited to what you can see with your user profile.

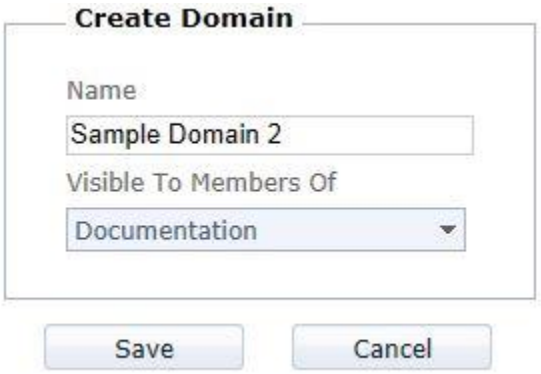

Figure 27 — Create Domain Example

(3) The domain will be created and appear in the list of domains and nodes in the left hand side of the display (see Figure 28).

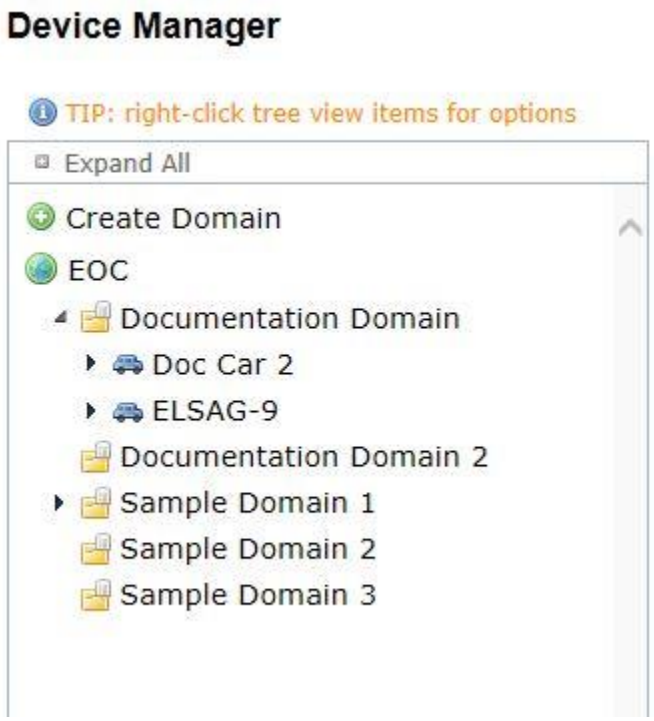

Figure 28 — List of Domains with New Domain

Now you can select the new domain and create the nodes that will define its organization.

5.2.4 Navigating the Device Manager Interface

Navigating the interface on the Device Manager page is simple. Use the scroll bar on the right side of the device manager tree to move up and down through the list. Click the arrow on a node in the tree that points to the right to expand that node and view its children. The arrow now points to the right & down. Click the arrow a second time to collapse it once again.

5.2.5 Node Command Options

In the left hand pane, right click to see the command options available for it (also see Figure 29). The options are:

- **Details**: Displays the details for the node to the right of the node tree.
- **Create**: Creates a new node as a child of the selected node.
- **Edit**: Edit the details for the selected node.
- **Delete**: Delete the selected node.
- **Export**: Exports the selected node to an XML file that is used to install CarSystem software for that node, or to install EOC software on a remote server as that node, and
- **Close**: Closes the command options menu.

Note: some options may be disabled, depending on the type of node selected.

5.2.6 Adding a Node

Each of the top-level nodes in your EOC implementation represents a domain that you have created in the EOC database. Your EOC installation comes with five default domains set up; one of the domains is named **Administrative**. See *Table D —Domains Created by Installer* on page 18 for a complete list of all domains created by the installer.

5.2.7 Adding a Node or Branch

You access the editing options for nodes in the Device Manager area by right clicking on an existing node. When you right-click, you will see the menu shown below in Figure 29. Then perform the steps that follow.

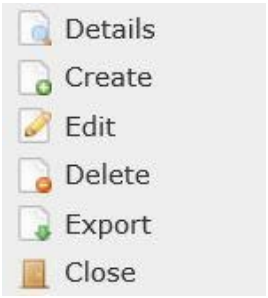

Figure 29 — Device Manager Edit Menu

(1) To add a node, select the existing node that you want to be the parent of the new node. For example, say you wanted to create a folder under **Sample Domain 2** named **West Side**.

(2) First, right-click on the **Sample Domain 2** node and select **Create**, as shown in Figure 30 below.

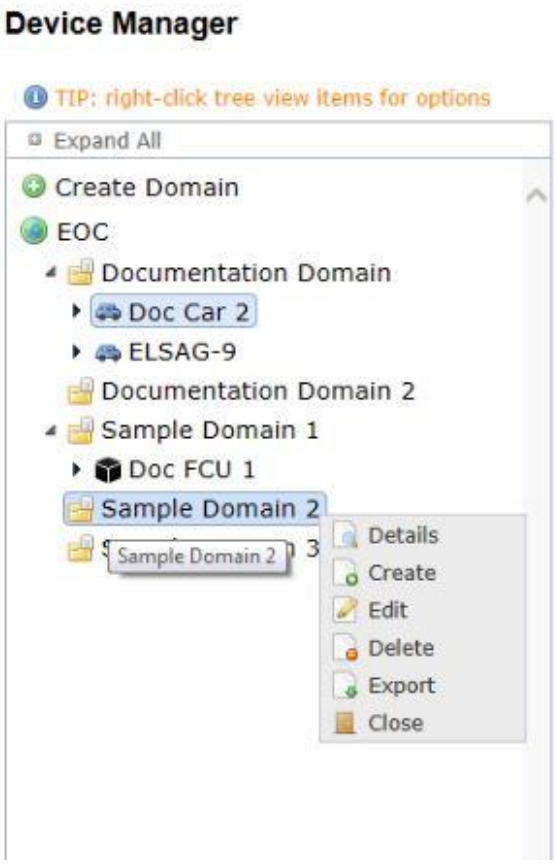

Figure 30 — Device Manager Initial Screen

(3) You will see the Create Item dialog prompt as shown in Figure 31 that follows.

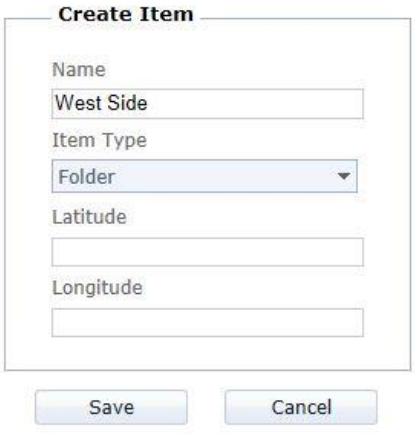

Figure 31 — Create Item Dialog

(4) Type **West Side** in the **Name** box and select **Folder** from the **Item Type** drop-down.

(5) **Latitude** and **Longitude** are optional entries. FCU fixed cameras which never move and do not have a GPS installed have their Latitude and Longitude entered one time at FCU CarSystem installation time. The coordinates then automatically populate the EOC entries.

(6) Press **Save**. Your newly created node appears in the tree where you created it as shown in Figure 32.

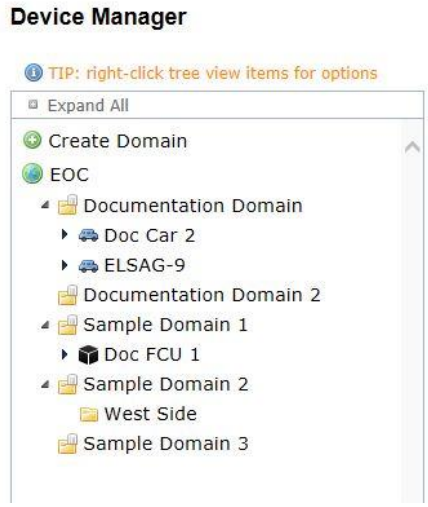

Figure 32 — Folder Created

5.2.8 Deleting a Node or Branch

Deleting a node or branch does not completely delete it from the database, since that would make all the associated historical data useless. Instead, the EOC makes the node or branch invisible when it is deleted.

(1) To delete, right-click on the node or branch you want to delete. (In this example, we are deleting the node we just created under **Sample Domain 2**.)

(2) Select **Delete**. You see the following warning message screen shown in Figure 33.

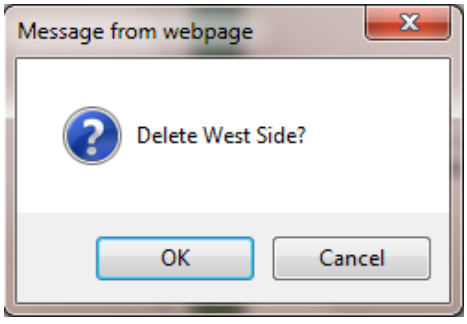

Figure 33 — Delete Node Warning Message

(3) Press **Cancel** to abort the delete if the command was executed in error.

(4) Press **OK** to delete the node. Referring to Figure 34 that follows, the deleted node is no longer visible.

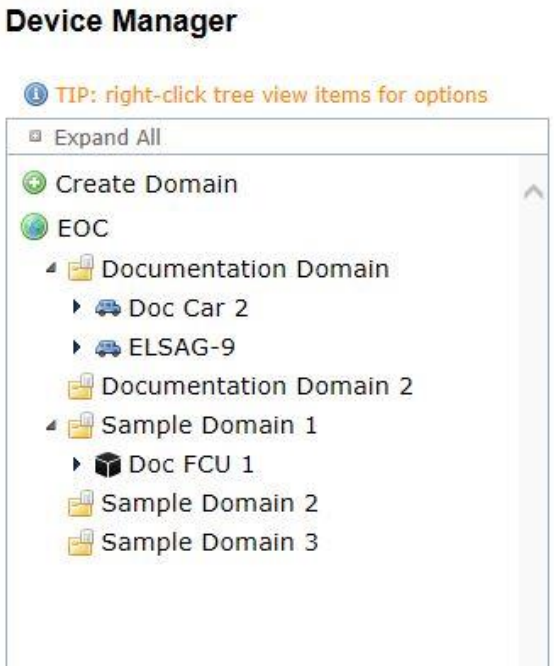

Figure 34 — Node Deleted

5.2.9 Viewing a Node

To view information about a node click on the node's name. You will see a display as shown in Figure 35.

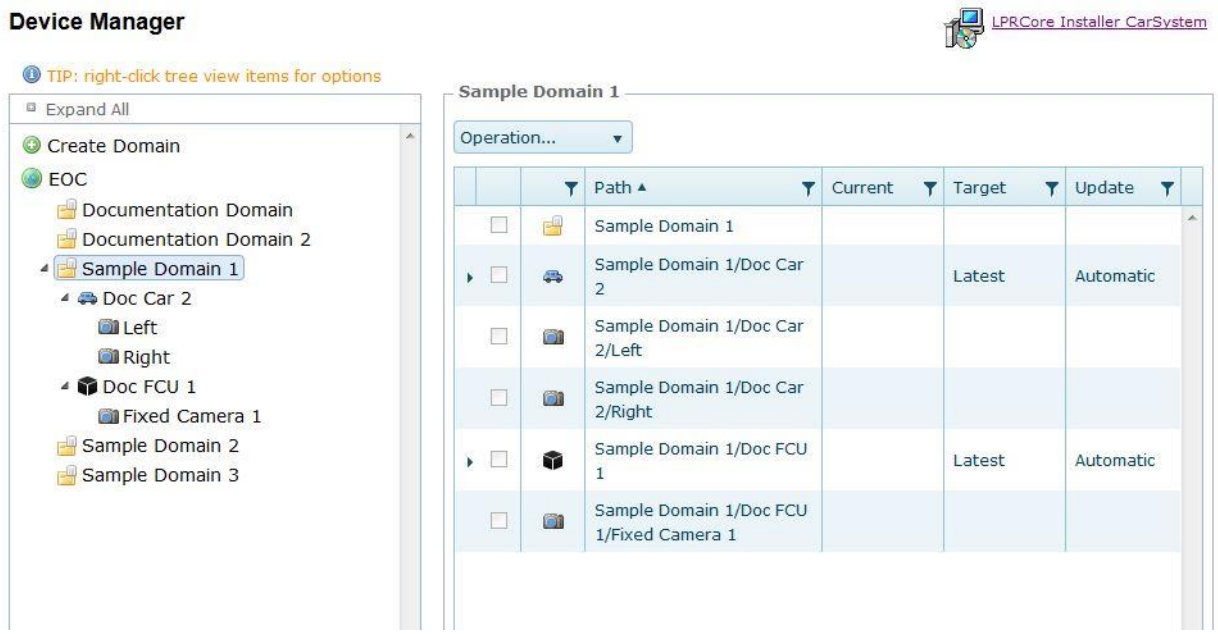

Figure 35 — View Node

5.2.10 Editing Node Information

To edit a node's information, right click on the node and select **Edit**. You will see the display shown in Figure 36. Change the information you want to change, and then press **Save**.

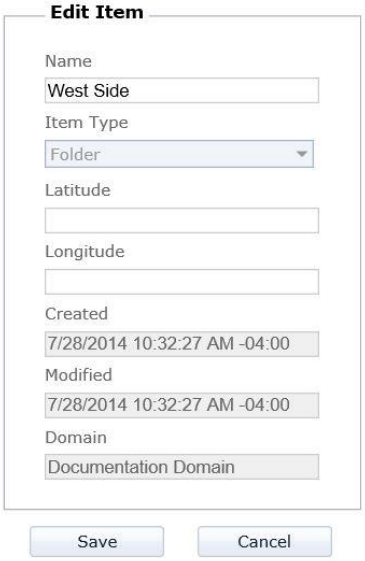

Figure 36 — Edit Node

NOTE: You cannot change the node's **Item Type** property.

5.2.11 Camera Names

By default, car or FCU CarSystem installations automatically detect the cameras that are installed and determines names for them from information on the camera. The cameras are automatically given names like Right, Left, Rear and Other. The person performing the installation has the option to leave the camera names at their defaults or assign a "friendly name" that is more descriptive. On FCU installations with fixed cameras pointing at specific lanes, the camera names can be changed to reflect the lane being observed. Examples could be "Highway 59 Left Lane", "Highway 59 Center Lane", and "Highway 59 Right Lane".

> **NOTE**: We recommend that cameras should only be added in the CarSystem application on the car or FCU. After installation and after the cameras appear in the EOC, the names can be changed in the EOC, which will then flow back out to the car or FCU CarSystem.

Note that the CarSystem camera configuration can be changed at any time by a user with the proper administrative privileges. See the *CarSystem User's Guide* for more information.

As shown in Figure 37, the FCU "Highway 59" has default camera named Left and Right. Follow the Edit Node instructions above to change the camera names. Repeat these steps to update all cameras that need to be updated.

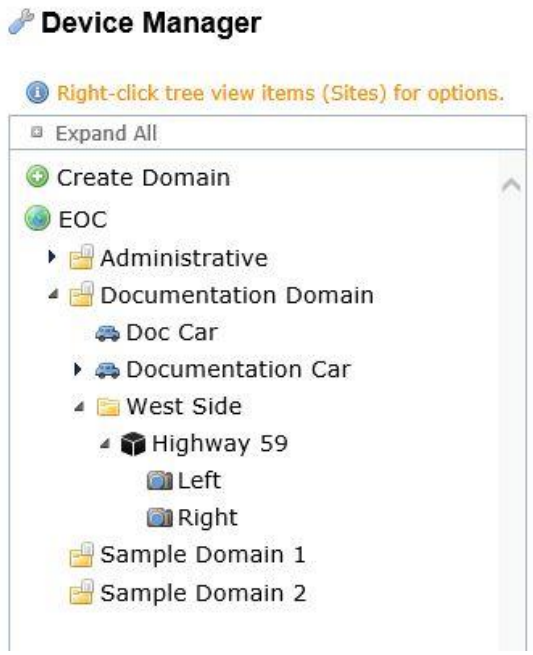

Figure 37 — FCU Default Camera Names

As shown in Figure 38, after editing the camera nodes, all cameras listed under Highway 59 FCU have friendly names. This will help when viewing Reads and performing Cross or Convoy Searches.

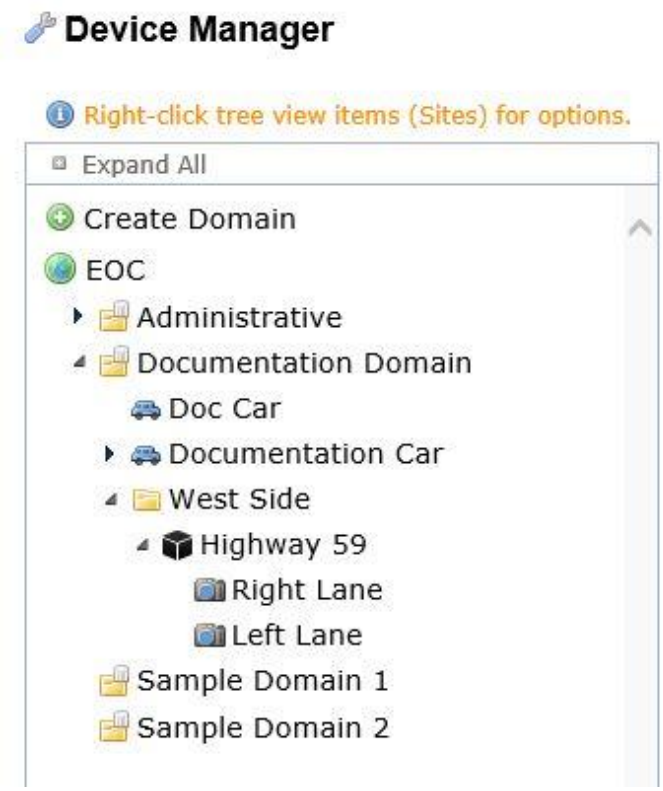

Figure 38 — Edit Camera Name

5.2.12 Exporting Node Information for CarSystem Installations

The **Export** command allows you to export system configuration information to a thumb drive or external storage device so that when you install CarSystem it will communicate correctly with the EOC.

You must perform this step before you install CarSystem, since the configuration information exported from EOC is necessary to install and configure CarSystem correctly. The output of the export process is an XML file that the CarSystem installation process can then read. The user can export in two ways, by exporting a single node and by exporting multiple nodes at one time

5.2.12.1 Export a Single Node

To export a single node use the following steps:

(1) Right-click on the node; you will see the display shown in Figure 39.

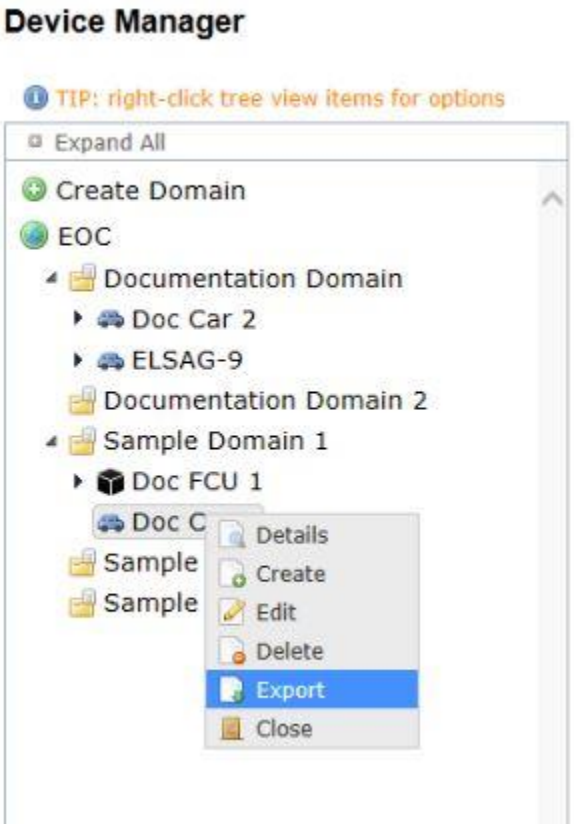

Figure 39 — Export Node Menu

(2) Select **Export**. The screen shown in Figure 40 is as it would appear if you are using Microsoft Internet Explorer.

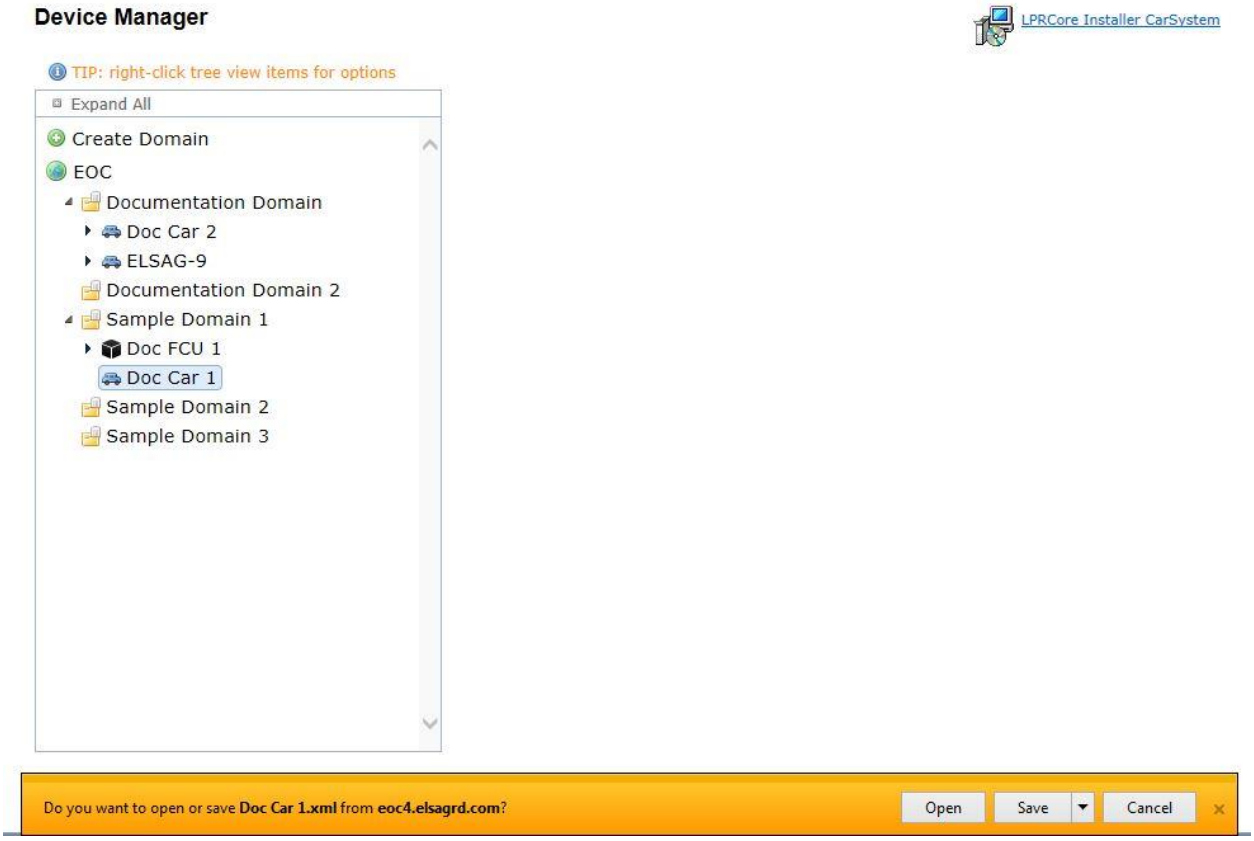

Figure 40 — Open or Save Node XML File

(3) Select **Save** and the file will be saved to your Downloads folder (in Windows 7).

NOTE: The prompt shown is the one generated by Internet Explorer. The prompt will look different if you use a different browser, like Firefox, Chrome, or even a different version of Internet Explorer.

(4) Copy the XML file to your USB stick or other drive for use in the CarSystem install.

5.2.12.2 Exporting Multiple Nodes at One Time

If you have created multiple cars or FCUs that will be installed all at once, you can export the XML files at the same time.

Referring to Figure 41, you want to export from Sample Domain 1 the car site named Doc Car 1 and the FCU named Doc FCU 1 at the same time. To do so:

(1) Click on the node named Sample Domain 1 to reveal the node details.

(2) Click on the Operations drop down and select **Export Sites**. The sites to be exported are automatically checked off. You can modify the selections manually.

(3) Once your selections are correct, click the **Export** button. A zipped file containing the XML files will be downloaded to your local PC.

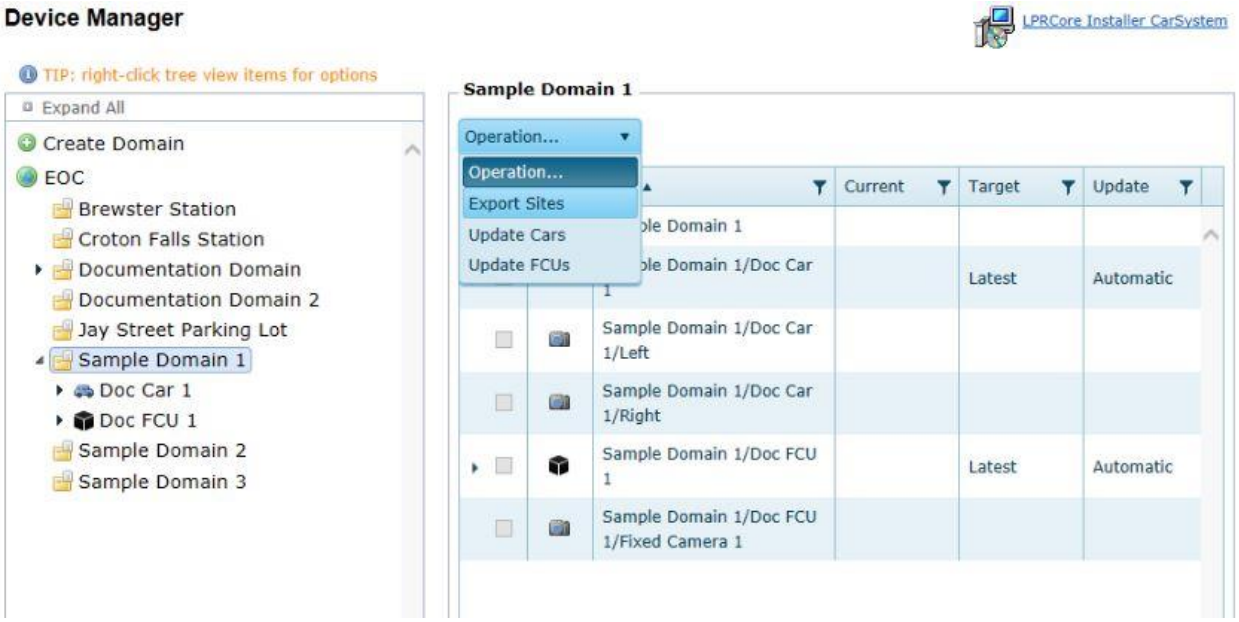

Figure 41 — Exporting Multiple Nodes at One Time

5.2.13 Moving Nodes from One Folder to Another

You can move Folder, Car, FCU and Server nodes from one folder to another folder in the Device Manager by dragging the node you want to move and dropping it in its new location. Domain and Camera nodes cannot be moved. The system will inform you if the move violates any system rules and will keep you from doing it if it will cause access difficulties.

5.2.13.1 Implications for Data

When you move nodes from one place to another within the EOC system configuration, you should be aware of the following potential effects of the move on the quality and integrity of the data stored in the database:

- The CarSystem and EOC user experience could change based on permission differences between the two domains. Visibility to the node, reads and alarms might be more or less restrictive.

- Any past reads or alarms generated by a car or FCU that is moved from one domain to another remain in the original domain. A grayed out entry for the car or FCU will appear in the Reader list in the **Data Mining > Query Reads** and **Data Mining > View Alarms** pages that can be used to limit the query results to that data.

NOTE: Deleting a node does not remove it from the database; it simply makes it invisible to the GUI. This is so that you can continue to search on and generate reports on historical data associated with that node.

5.2.14 Upgrading Car and FCU CarSystem Software

When the EOC is upgraded to a new version it is advisable to upgrade all cars and mobile units to the latest version as soon as possible. There are two ways to upgrade remote devices: manually and automatically from the EOC.

NOTE: Earlier versions of CarSystem Mobile and CarSystem Fixed (6.6 and lower) will not auto-upgrade and have to be upgraded manually.

5.2.14.1 Manual Upgrades

Manual upgrades require someone to physically move a copy of the LPRCore Installer CarSystem.msi installer file from the EOC to the remote site and run the installer on that device. This could be by remote access or physically visiting the remote site.

To access the LPRCore Installer CarSystem.msi installer file, perform the following steps:

(1) Log into the EOC.

(2) Select **System > Device Manager**.

(3) Referring to Figure 42, on the Device Manager page, click the LPRCore Installer CarSystem link.

Figure 42 — LPRCore Installer CarSystem Link

(4) You will be asked where you want to save the file. Select a location and click Save.

If the remote site has remote access, perform the following steps:

(1) Connect to the remote site.

(2) Copy LPRCore Installer CarSystem.msi installer to the site's PC.

(3) Run the installer on the remote site.

If the remote site does not have internet access to the EOC, perform the following steps:

(1) Follow the above steps from a computer that has access to the EOC and save the installer to a thumbdrive you can bring to the remote site.

(2) At the remote site run the installer and upgrade the existing CarSystem software.

5.2.14.2 Automatic Upgrading from an EOC

EOC 5.1 and later Device Manager allows the automatic upgrading from the EOC of a remote site (car or FCU) as long as the remote site has a wired or wireless connection to the EOC. Follow these steps to initiate the remote site upgrades:

(1) You can select one or multiple sites to upgrade at the same time. Referring to Figure 43, to upgrade one remote site select that single car or FCU in the left panel. If upgrading multiple cars or FCUs select the top of the node you want to upgrade. In the below example all sites under node **Documentation Domain** will be displayed on the node detail view.

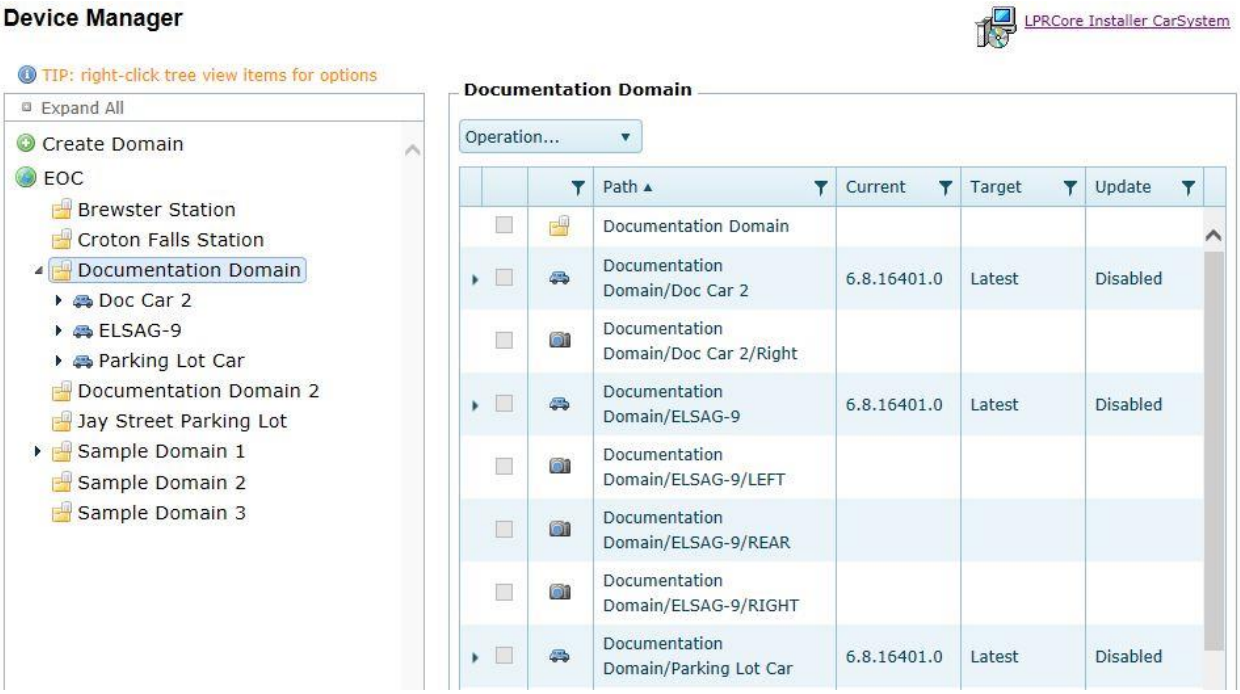

Figure 43 — Documentation Domain Example

(2) Referring to Figure 44, select the **Operation** dropdown and then either **Update Cars** or **Update FCUs**. The sites to be upgraded will automatically be checked as shown in Figure 44.

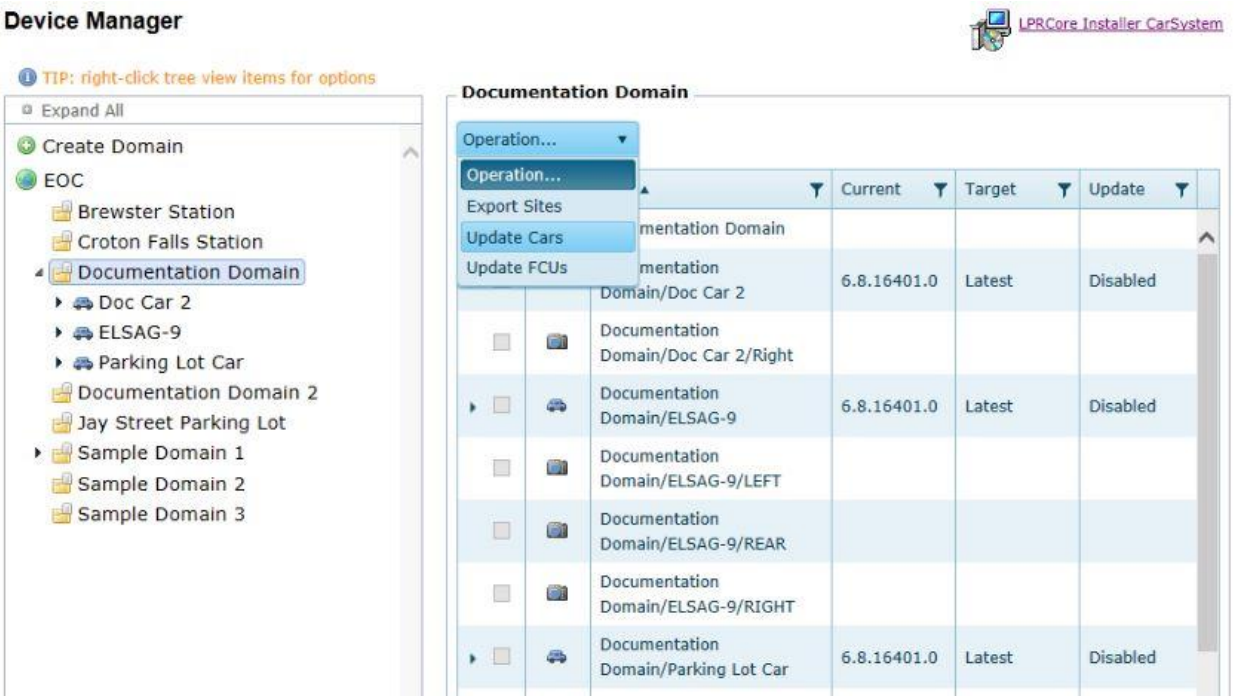

Figure 44 — Operation Dropdown

(3) Referring to Figure 45, select the **Target Version** dropdown and select **Latest**.

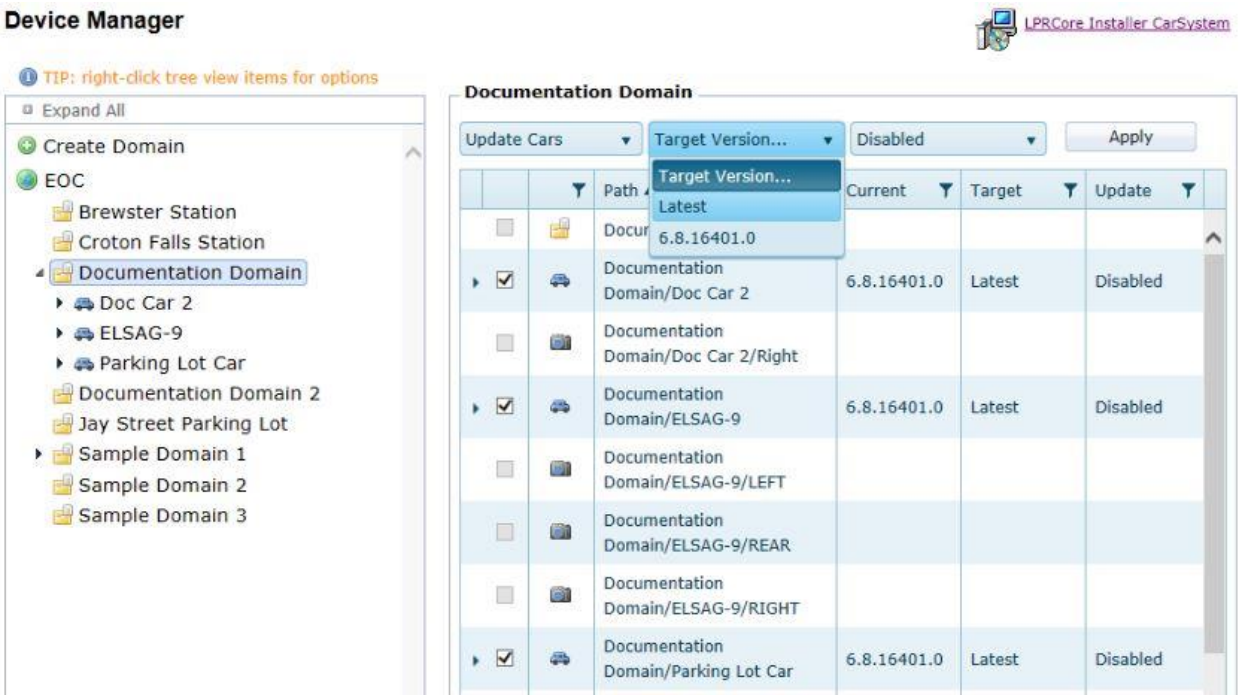

Figure 45 — Target Version to Latest Version

(4) Referring to Figure 46, select the **Update Type** dropdown and select **Automatic**.

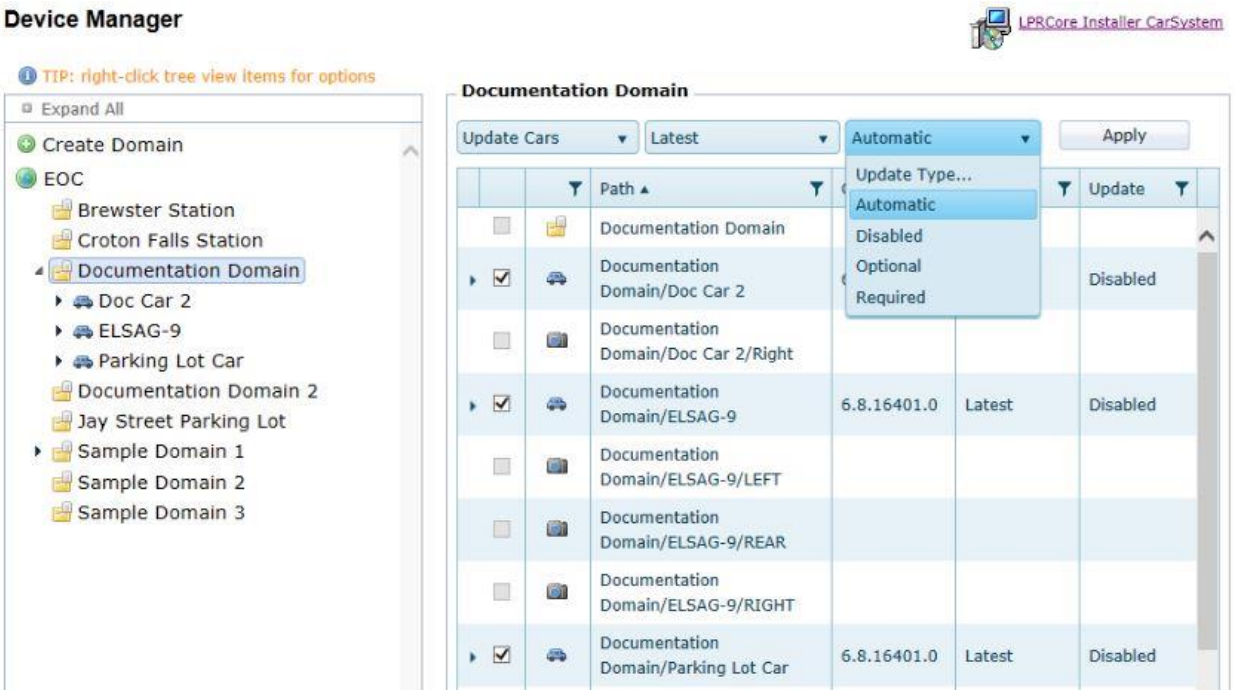

Figure 46 — Update Type to Automatic

Update Types:

- Automatic – CarSystem updates will be pushed to the remote device (car or FCU) and update without user intervention, even if the CarSystem UI is not running.
- Disabled – No CarSystem updates will be pushed to the remote device.
- Optional – When the CarSystem UI is run by a user, the user is alerted that an update exists but must acknowledge and initiate the start of the update. They can delay the update indefinitely unless they say yes.
- Required – When the CarSystem UI is run by a user, they must run the update or CarSystem closes

(5) Referring to Figure 47, if all options are correct, click **Apply**.

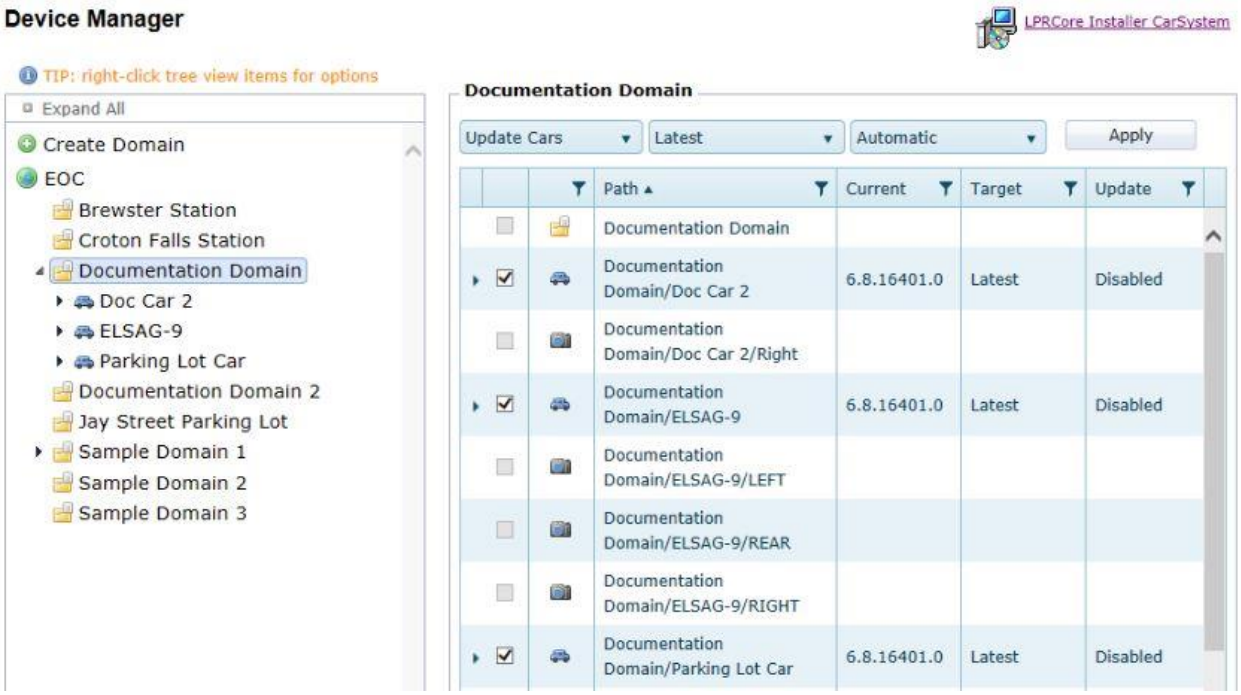

Figure 47 — Review Documentation Domain Settings

(6) Referring to Figure 48, you will be asked to confirm the number of remote sites that will upgrade.

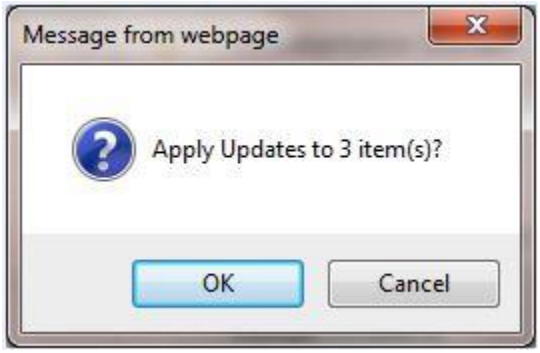

Figure 48 — Apply Updates Confirmation

At this point the EOC will start transmitting the LPRCore Installer CarSystem.msi installer to the remote site. Network bandwidth from the EOC and at the remote site determines how long it will take for the sites to finish the upgrade. When the sites are upgraded Device Manager will display the version number in the **Current** column.

5.2.14.3 Considerations

It is best that the remote site knows an upgrade is being pushed down to them. If a CarSystem is running at upgrade time, the CarSystem process will be killed so that the upgrade will proceed. That might interrupt a deployed patrol car.

Time the upgrade for off-peak hours if down time or Internet bandwidth is a concern.

Outgoing network bandwidth speed might be affected if upgrading many remote sites at one time.

> **NOTE: Effective EOC 5.4 and CarSystem 6.10.x:** The CarSystem database is completely replaced during an upgrade from CarSystem 6.9 or earlier to CarSystem 6.10 or later, resulting in no historical data residing on the remote FCU or mobile unit. Ensure that all previous data has transferred to the EOC before initiating any upgrade.

5.3 System Tasks

The **System Tasks** selection allows you to view the available system management tasks, schedule them and run them. Running these tasks ensures better EOC system and database performance, so you should either schedule them to run automatically or be sure to run them on a regular basis.

All new EOC installations have default tasks for Database Maintenance and Data Retention, which should be scheduled to run daily. Midnight is the default time. Also, note that you must have permissions to see the tasks. Refer to Figure 49 and the steps that follow:

(1) Select **System** > **System Tasks**. You will see the screen shown in Figure 49, which shows the characteristics of each of the system tasks available to you.

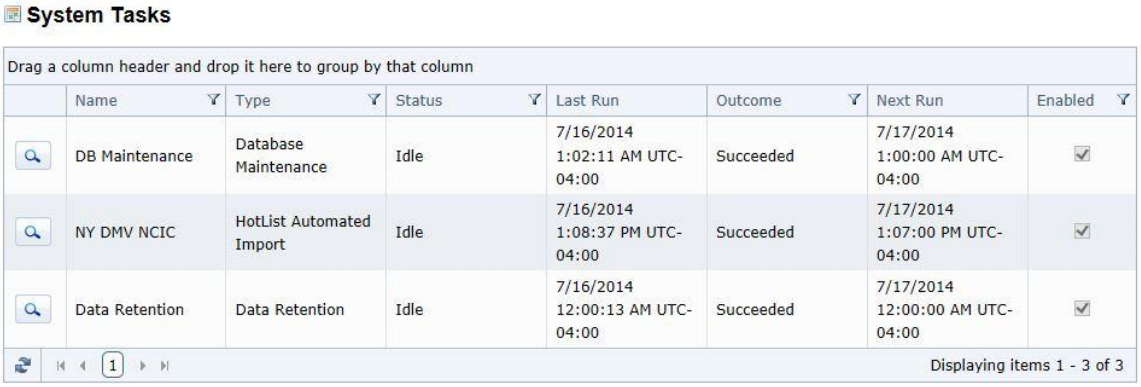

Figure 49 — System Tasks List

If you have automated a List Import you will also see it listed here. As shown in Figure 49, NY DMV NCIC is automated to be imported daily at 1:07 PM.

Note that these tasks all take some finite amount of time to run. How long each runs depends on how much data it has to process. In order to keep from overloading the system, it is best if tasks are scheduled at different times.

(2) Select **Details** (magnifying glass icon) to view or edit the details of the task, including its schedule. See Figure 50.

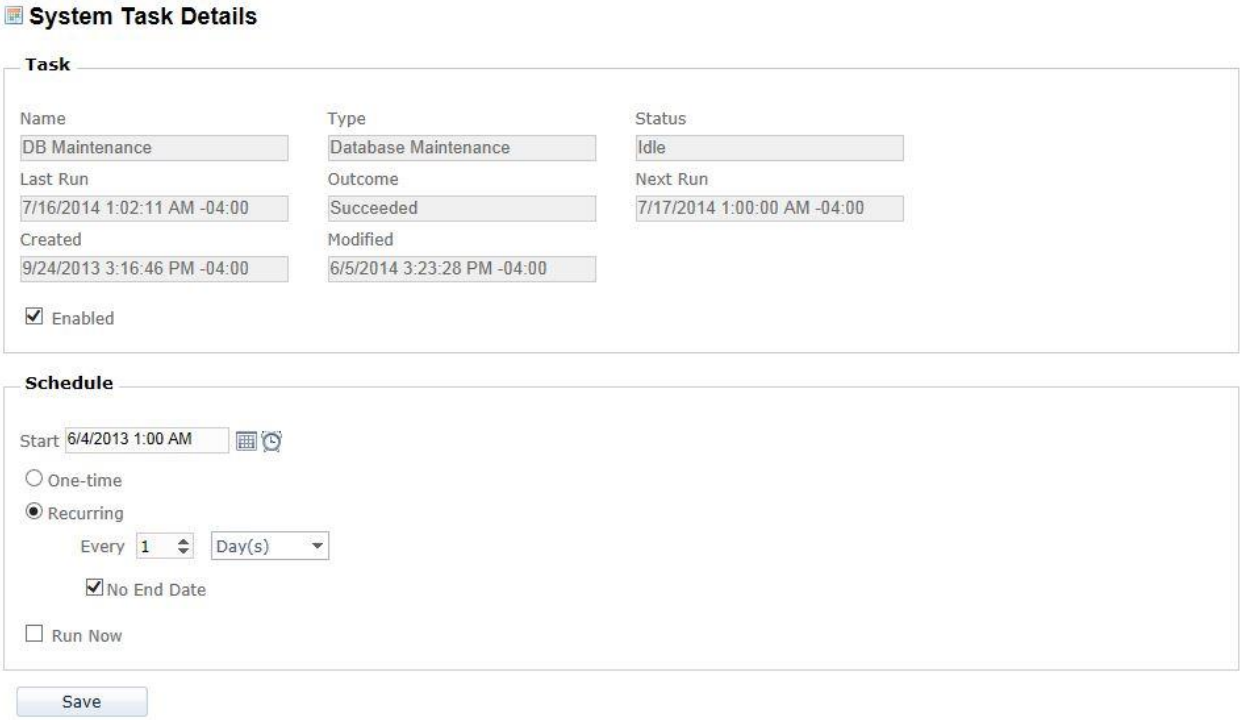

Figure 50 — System Tasks Details

(3) If you have the appropriate permissions, you can change the schedule or other characteristics of the task, including **Start** time, whether the task should be run **One-time** or on a **Recurring** basis, and the day and time a recurring task should run.

NOTE: To alter the date, click on the calendar icon and select the date to run the task; to change the time, click on the clock icon and set a time.

(4) Press **Save** to save any changes.

5.4 Application Settings

5.4.1 Accessing Application Settings

Application Settings are accessible by selecting *App Settings* from the *System* menu. If the logged in user does not have the App Settings feature permission, this menu item will not be visible.

Additionally, starting with EOC release 5.6 **Application Settings** cannot be accessed unless the user is connected to the EOC at http://localhost on the web server itself. This is for increased security and to make sure that changes that are saved actually take effect. Figure 51 below shows the message that is displayed if you navigate to the Application Settings page using a web browser running on a machine other than the one on which the EOC web app software is installed.

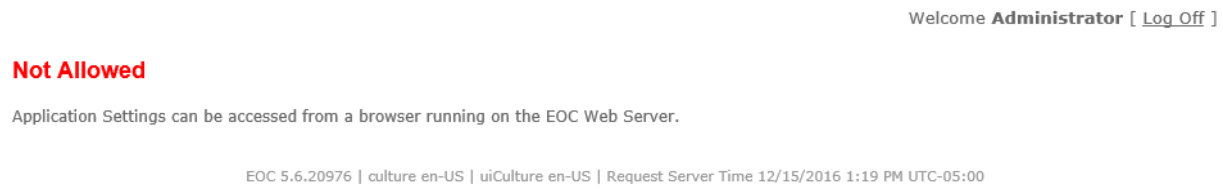

Figure 51 — Application Settings Not Allowed Message

Figure 52 shows the Application Settings page if you navigate to it using a browser running on the machine on which the EOC web app is installed.

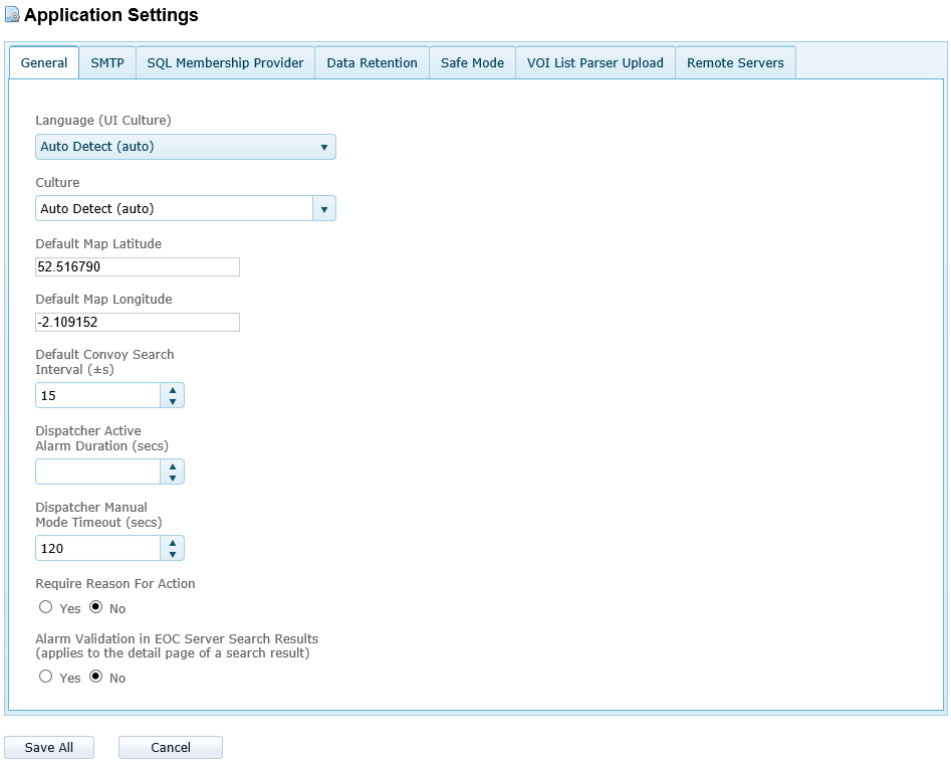

Figure 52 — Application Settings Page

The tabs across the top of the page are discussed in turn below.

5.4.2 General

Contains settings that apply to all areas of the EOC.

5.4.2.1 Language and Culture

The Language setting determines the language in which the EOC will be displayed. Supported languages selections are English (United States), English (United Kingdom), Spanish (Chile) and Malay (Malaysia).

The Culture setting determines the formatting of dates, times, currency and large numbers. Any culture that can be selected from Windows Region control panel is supported.

If either setting is **Auto Detect**, the setting is taken from the browser.

If Spanish (Chile) is selected, the EOC will appear in Spanish for all users regardless of browser setting. If all EOC users are Spanish-speaking (whether in Chile or not) the Language selection should be Spanish. For a mix of English- and Spanish-speaking users, the Language selection should be Auto Detect. Each user's browser settings will determine the language in which the EOC appears.

If Malay (Malaysia) is selected, the EOC will still appear in English; but the sounds that are played in Dispatcher when an alarm occurs will be spoken in Malay.

5.4.2.2 Default Map Latitude and Longitude

Sets the default map location (center point) when maps are first displayed. Applies to Query Reads, View Alarms, Cross Search, Convoy Search and Dispatcher.

5.4.2.3 Default Convoy Search Interval

Sets the default plus or minus time Convoy Search uses (in seconds).

5.4.2.4 Dispatcher Active Alarm Duration (secs)

Specifies the default time period Dispatcher uses to keep a recent alarm active when it is in Automatic Map Mode. This helps when an alarm is delayed from reaching the EOC in a timely manner.

5.4.2.5 Dispatcher Manual Mode Timeout (secs)

Specifies the length of the timeout period that Dispatcher waits to switch from Manual Map Mode to Automatic Map Mode.

5.4.2.6 Require Reason for Query

For auditing purposes, anytime a user queries reads or alarms a reason for the query or export must be given. The reason is saved with the Audit message for the action.

5.4.2.7 Alarm Validation in EOC Server Search Results

When enabled, Alarm validation (marking an alarm as correct or incorrect) can be performed at the EOC server level by authorized users using the Reads/Alarms detail page. Alarms can always be validated by authorized users in Dispatcher.

5.4.3 SMTP

When EOC was installed, the process asked for SMTP settings to configure how EOC would send emails such as password notifications to new users, etc. You can change these settings in this SMTP section.

5.4.3.1 From Address

The string entered here will appear in the From: field in emails sent by EOC.

5.4.3.2 SMTP Server

The address of the SMTP server that the EOC will use to send emails.

5.4.3.3 Port

The port the EOC will use when communicating with the SMTP server.

5.4.3.4 Authentication Settings

The authentication information the EOC will use when it connects to the SMTP server.

5.4.3.5 Send Test Email To

When you change the settings, click on the **Test** button and EOC will send a test email to this email address to confirm they are correct.

5.4.4 SQL Membership Provider

This section allows the setting of password constraints for EOC running under SQL Server Membership:

5.4.4.1 Maximum Invalid Password Attempts

A user will be locked out if they enter the wrong password more than this number of times within the window specified by **Password Attempt Window (minutes)**.

5.4.4.2 Password Attempt Window (minutes)

Specifies the length of the window within which entering invalid passwords while logging in causes the user ID to be locked.

5.4.4.3 Minimum Required Password Length

Specifies the shortest allowed length of a password in characters. Requiring longer passwords helps to make user passwords more secure.

5.4.4.4 Minimum Required Nonalphanumeric Characters

This setting indicates the minimum number of symbol characters that must be present in a password. Including symbol characters helps make a password stronger and harder to guess.

5.4.5 Data Retention

Data Retention parameters are options for setting how many days data is retained/stored in EOC. Users might have different data retention policies for reads or alarms based on local statutes or policies.

Referring to Figure 53, Data Retention can be enabled for the supported data types:

- If there are no limits on Data Retention, uncheck all the Enabled checkboxes.
- Audit Messages, Log Messages and Reads can have their own Data Retention values.
- Alarm retention can be limited in two ways:
  - If all Alarm Types have the same retention policy, select the "All Alarm Classes" checkbox and set the number of days.

- If different Alarm types have different retention policies, make sure the "All Alarm Classes" checkbox is not selected. Then "Enable" and set each Alarm Type to the appropriate number of retention days.

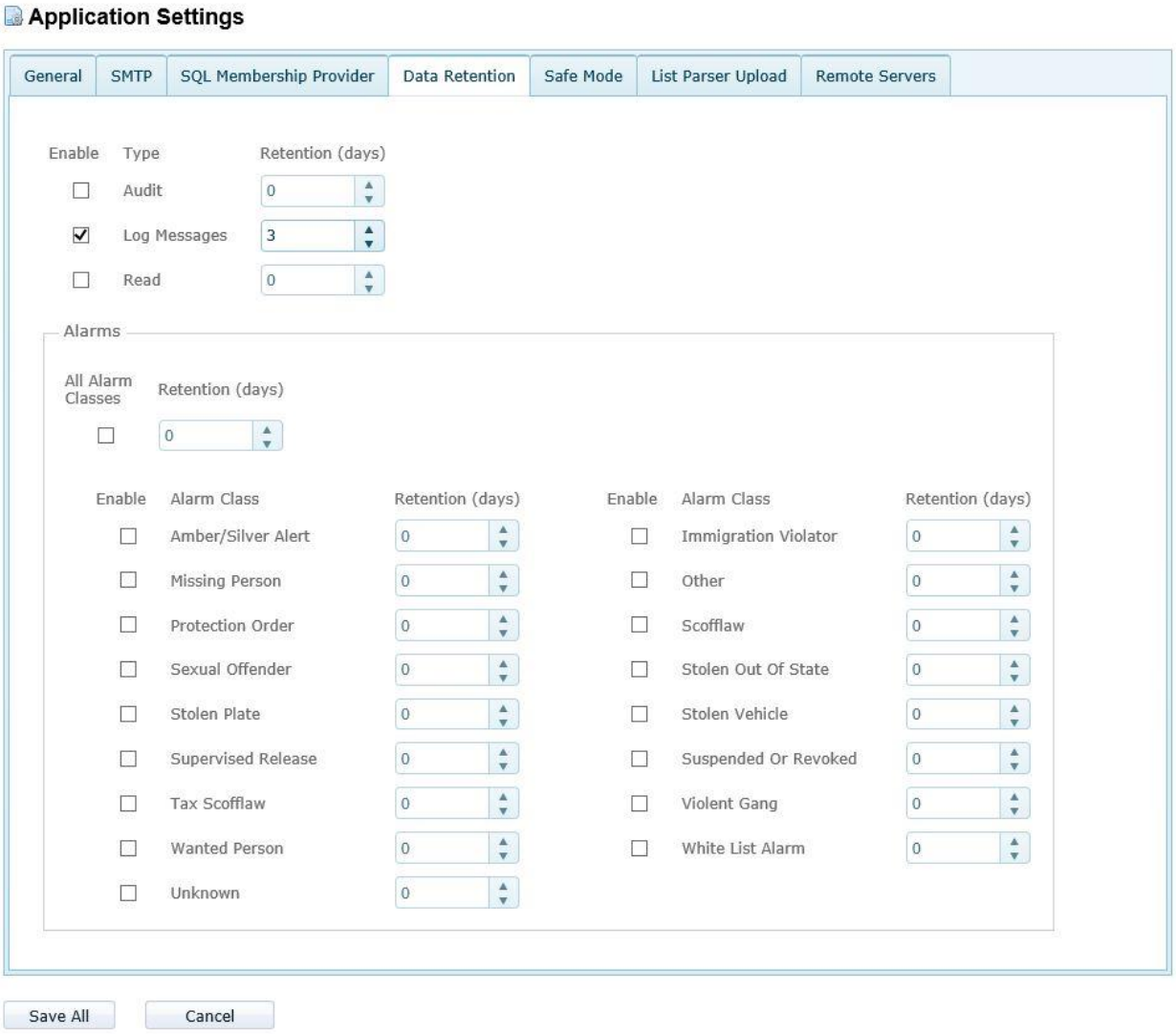

Figure 53 — Data Retention

5.4.6 Safe Mode

Using Safe mode is described in the ***Safe Mode*** section on Page 79.

5.4.7 List Parser Upload

Allows the upload and saving of a compiled custom list parser supplied from Selex ES. List Parser Upload also displays the parsers that are currently installed, including both custom parsers and the default parsers included with the EOC. Custom parsers can be deleted; default parsers cannot.

5.4.7.1 Default Parsers

By default, the EOC includes parsers for CSV (comma separated values) formats for several alarm classes as well as a parser for the Elsag Legacy Format. The CSV parsers import CSV files consisting of three "fields": License Plate; State; and an optional comment. The Elsag Legacy Format is described in more detail below.

5.4.7.1.1.1 Elsag Legacy Format

Referring to the bullets and Figure 54 that follow, the Elsag Legacy List format is a fixed-length format, meaning that each field is always the same length. Details about the required parameters are as follows:

- The "PLATE" is an alphanumeric string of up to eight characters. If the plate string length is less than eight, "SPACE" characters must be added to fill the remaining positions (up to a total of eight). Only upper case letters are allowed. No special characters are allowed, only 0 to 9 and A to Z.
- The "STATE" is an alphabetic string of always two characters. No digits are allowed.
- The "ALARM CLASS" is a string of up to two characters that matches one of the Alarm Class List values below, and
- Any string from position 12 to the end of the line is considered as "COMMENT" information.

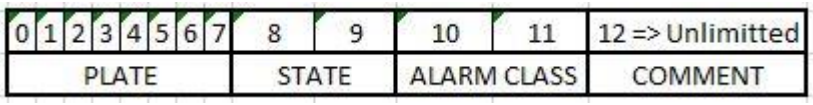

Figure 54 — ELSAG Legacy List Detail

Below is the ELSAG Legacy Alarm Class List sorted by ID and Description (# is required):

#0	Unknown
#1	Stolen Vehicle
#2	Wanted Person
#3	Stolen Plate
#4	Suspended Or Revoked
#5	Scofflaw
#6	Stolen Out Of State
#7	Violent Gang
#8	Sexual Offender

#9 Other

NOTE: A "single digit" Alarm ID (left column) needs a leading number (#) sign. The Elsag Legacy Format parser does not support Alarm Classes 10 & up.

5.4.7.2 Custom Parsers

A custom parser can be created to import List data in any text-based format. Contact Selex-ES Inc. to obtain a custom parser.

5.4.7.3 List Upload Scripts

Lists can be imported in either of two ways. A single List file can be imported by selecting Lists > List Upload. This process is described in more detail in the *EOC User's Guide*.

Alternatively, a script can be used to automate the List upload process. A script tells the EOC which parser to use and where to look for List file(s) to upload. Scripts, if used, are specified when a List is created or updated under Lists > List Names. When a List is automated with a script, a System Task is added, as described in System Tasks above.

It is necessary to upload Lists using a script if the List data is distributed across more than one file. It may be preferable to upload Lists using a script depending on how you receive List updates.

Whether a List is updated by directly importing a file or by using a script, the internal process is the same, as described in the *EOC User's Guide*.

5.4.8 Remote Servers

Allows the entry of remote server information which allows the EOC to subscribe to and search another EOC's information.

Setting up Remote Servers is described in detail in the ***Data Sharing*** chapter.

6 Data Sharing

6.1 Data Sharing

The Data Sharing feature allows your organization to share data with other organizations. This is useful in counter terrorism operations and other cases where inter-agency cooperation is required. There are two alternative modes of operations:

- **Search Data** (formerly Linked server): In this case the client EOC user can run queries against a remote EOC server. Data stays on the remote EOC and nothing is physically moved.
- **Copy Data** (Data Sharing Mode): Data is actually replicated from a satellite EOC to a main host which aggregates data from multiple smaller EOCs.

The EOCs involved in the data sharing relationship are distinguished based on their roles:

- **Subscriber:** This is the EOC which either runs the **Search Data** remote query or receives **Copy Data** from a remote EOC.
- **Publisher:** This is the EOC that either answers to a **Search Data** query from a remote EOC or sends its own data to a remote aggregation center.

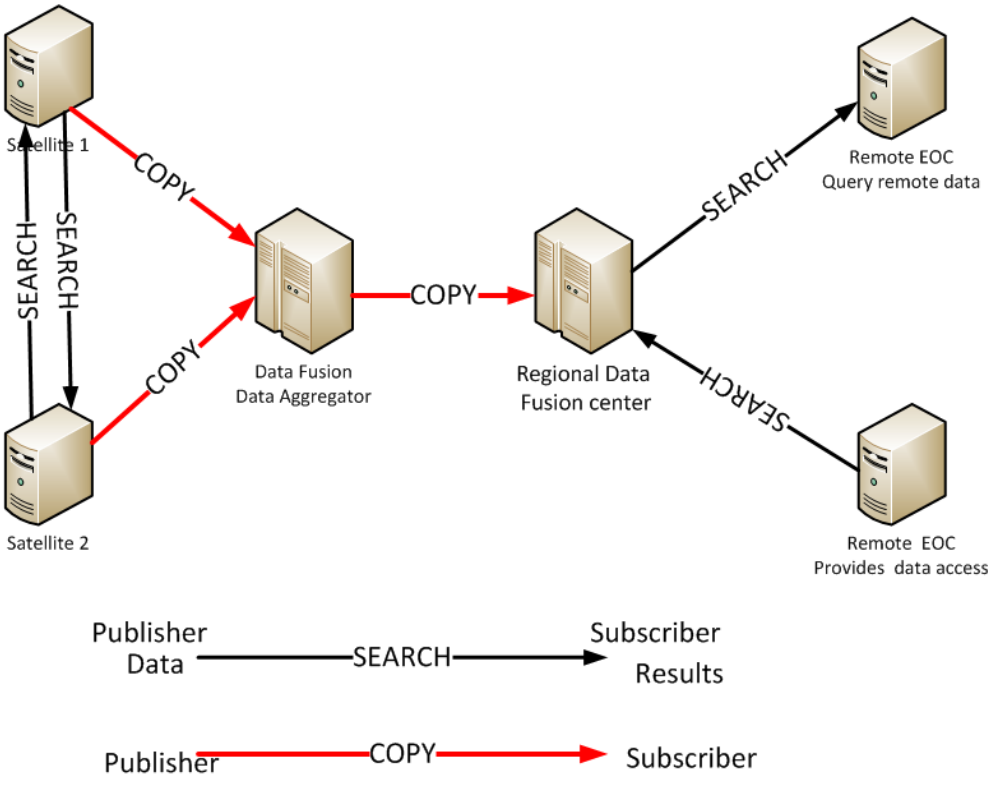

Figure 55 — Data Sharing Data Flow

The Publisher EOC can share reads and alarms with its subscriber EOCs. Sharing plate lists, users, groups, domains and sites between EOCs is not supported.

Data is shared by domain. That is, the publisher EOC only publishes reads and/or alarms in specific domains to its subscriber EOCs.

6.2 Setting up Search Data Sharing

Certain steps need to be completed on the Subscriber and Publisher EOCs in order to establish the connection for searching data. Below is a summary of those steps:

Table H — Setting up Search Data Sharing

Step	Subscriber	Publisher
1	Create a connection to the remote EOC database that will be queried. Needs connection info from the remote agency EOC.	
2	Create a Domain and a Device Manager Server Node representing the Publisher (the remote EOC)	
3	Export server node configuration XML file.	
4	Send the XML file to the remote agency administrator (handshake, approval)	Receives the XML file and determines what data domain to expose
5		Creates a server node representing the remote subscriber and loads subscriber XML file
6		Repeat step 5 for all other domains to be shared
7	As soon as the xml file is loaded it will be possible to run remote queries	

6.2.1.1 Search Data Sharing Steps

Starting on the Subscriber EOC:

(1) Navigate to the **System > App Settings** page, then switch to the **Remote Servers** tab

(2) Create a connection to the remote EOC database that will be queried. Click **Add New Record**.

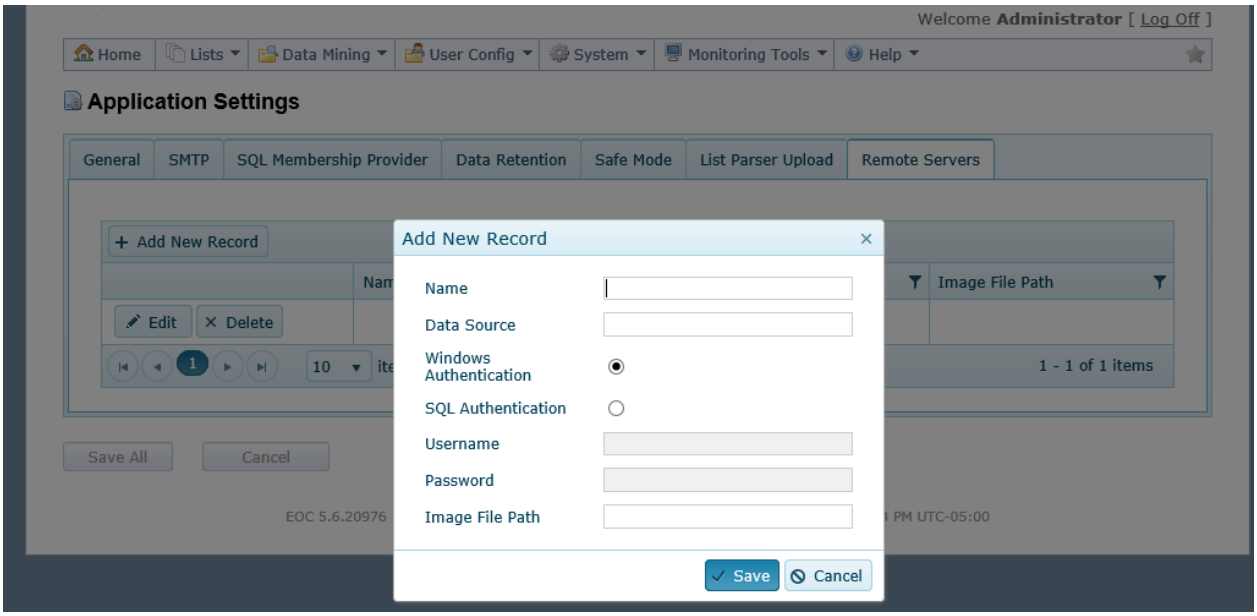

Figure 56 — Remote Server Setup

Remote Publisher Server information must be provided by the administrator of that EOC. The following information is required:

- **Name**: Friendly name of the connection. This will be used to identify the remote link.
- **Data Source**: The name or IP address of the remote Publisher EOC's SQL Server machine.
- **Windows** or **SQL Server Authentication**: Information needed to access the Data Source. This is the same info used when setting up the old linked server.
- **Image File Path**: Exact path on the remote server where the images are stored.

(3) Select the **System > Device Manager** page.

(4) Create or use an existing Domain and create a Server node for the remote EOC database that will be queried. The name you enter will be the name of the Publisher EOC in the Subscriber EOC's User Interface.

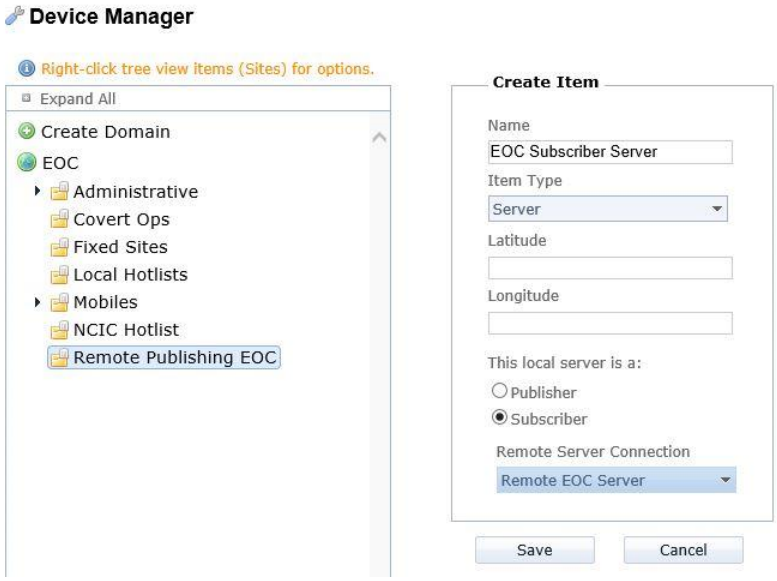

Figure 57 — Subscriber Server Node Setup

- Enter the **Name** for the Publisher EOC that is displayed on the Subscriber EOC.
- Change Item Type to **Server**.
- Change "This local server is a:" to Subscriber.
- Under **Remote Server Connection**, select the Publishing Server name.
- Click **Save.**

(5) On the Subscriber EOC, export the server node XML. Right click the node created in Step 2 and select the **Export** option.

(6) Send the exported XML file to the remote EOC administrator.

Next, on the Publisher EOC:

(1) Create a server node within the Domain to be exposed to the Subscriber EOC. Reads and alarms of the selected domains will be searchable by the Subscriber.

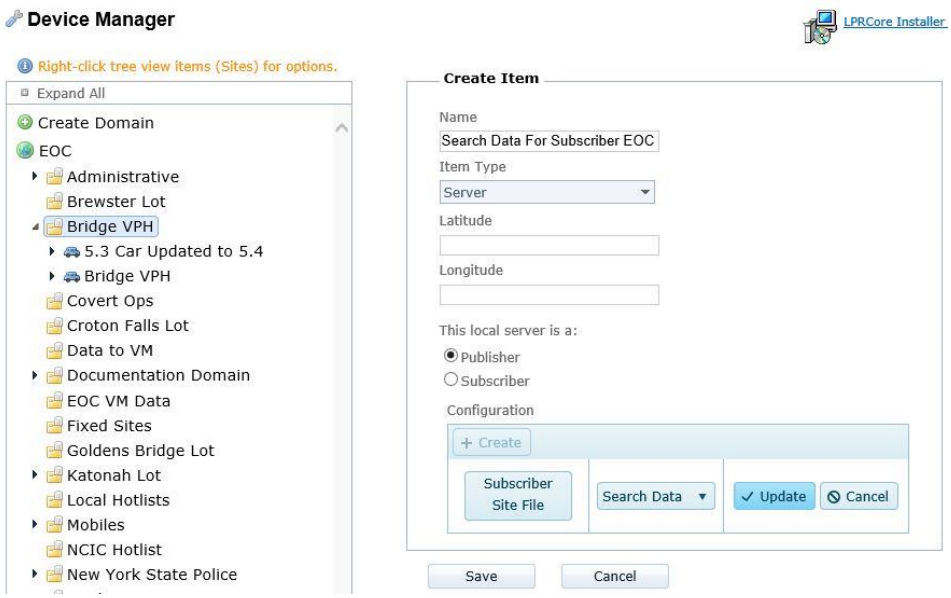

Figure 58 — Publisher Setup of Subscriber

- Enter the **Name** for the Subscriber EOC in the Publisher EOC.
- Change Item Type to **Server**.
- Change "**This local server is a:**" to Publisher.
- Click **+Create**
- Change **Copy Data** drop down to **Search Data**.
- Click **Subscriber Site File**.
- Browse to where the Subscriber XML file is located and select it
- Click **Open** to use the file with this node.

(2) Click **Update** to save the configuration.

(3) Click **Save.**

(4) Repeat Steps 1 through 3 for all Domains that will be shared with the Subscriber.

6.2.2 How Data from the Publisher Is Displayed By the Subscriber

- On the Data Mining pages, the Publisher server node name shows up in the **Reader** column.
- The actual name of the FCU/Car and camera will show up on the **Read Detail** page. These will be the names from the Publisher system and so will not be known on the Subscriber server.
- If a Subscriber receives reads from a remote domain and some of the reads match a List on the Subscriber there will **NOT** be any local alarm because in our current system List matching is performed exclusively by CarSystem and not by the EOC webserver software.

6.3 Setting up Copy Data Sharing

Certain steps need to be completed on the Subscriber and Publisher EOCs in order to establish the connection for Copy Data. Below is a summary of those steps:

Table I — Setting up Copy Data Sharing

Step	Subscriber	Publisher
1	Create a connection to the remote EOC database that will be queried.	
2	Create a Domain and a Device Manager Server Node representing the Publisher (the remote EOC). Data will be local but associated to this virtual Reader. (Remote database connection info is left blank).	
3	Export server node configuration XML file.	
4	Send the XML file to the remote agency administrator (handshake, approval)	Receives the XML file and determines what data domain to expose
5		Creates a server node representing the remote subscriber and load subscriber XML file using Copy Data mode.
6		Repeat step 5 for all other domains to be shared
7	As soon as the xml file is loaded by the Publisher the EOC will start receiving actual metadata and images through LPRCore to LPRCore communications.	Restart web server LPRCore_agg service to enable the changes.

6.3.1.1 Copy Data Sharing Steps

Starting at the **System > Device Manager** tab:

(1) On the Subscriber EOC, create or use an existing Domain and create a Server node for the remote EOC database that will be queried. The name of the Server node will be the name of the remote node (Publisher) in the User Interface.

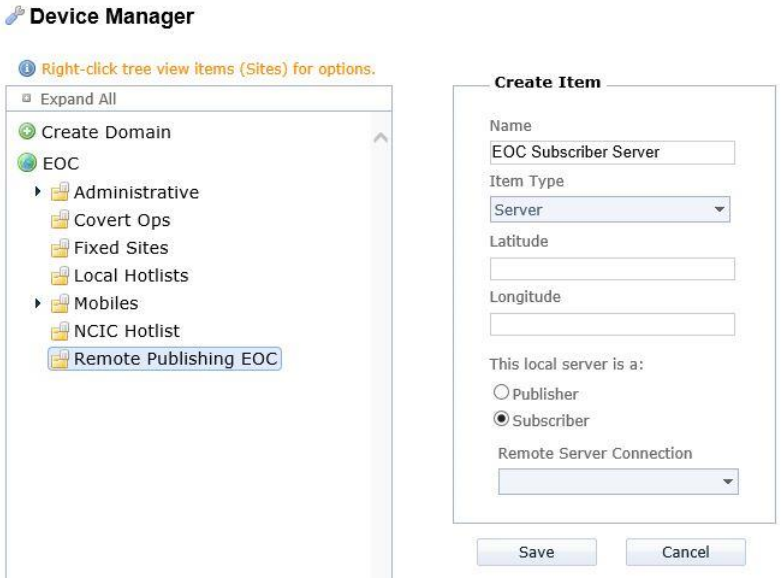

Figure 59 — Subscriber Server Node Setup

- Enter **Name** for Subscriber EOC.
- Change Item Type to Server.
- Change "This local server is a:" to Subscriber.
- Under **Remote Server Connection**, nothing needs to be selected.

(2) Click **Save.**

(3) On the Subscriber EOC, export the server node XML. Right click the node created in Step 2 and select the **Export** option.

(4) Send the exported XML file to the remote EOC administrator.

(5) On the Publisher EOC, create a server node within the Domain to be exposed to the Subscriber EOC. Reads and alarms of the selected domains will be searchable by the Subscriber.

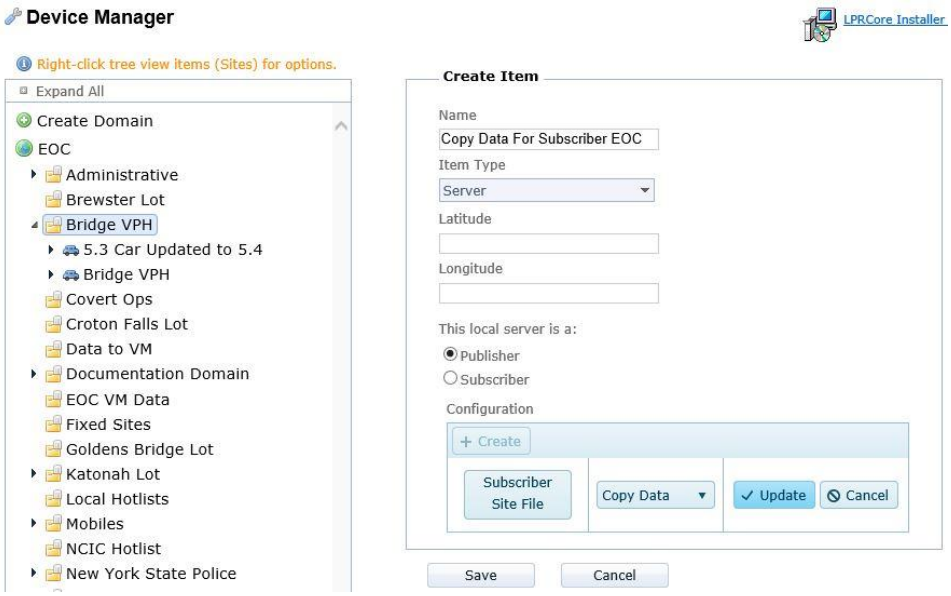

Figure 60 — Publisher Setup of Subscriber

- Enter **Name** for Subscriber EOC.
- Change Item Type to Server.
- Change "This local server is a:" to Publisher.
- Click +Create
- Leave **Copy Data** drop down as **Copy Data**.
- Click **Subscriber Site File**, browse to where the Subscriber XML file is located, Click **Open** to save.

(6) Click **Update** to save Configuration.

(7) Click **Save.**

(8) On the Publisher EOC, repeat Step 5 for all Domains that will be shared with the Subscriber.

(9) On the Publisher EOC, restart the EOC webserver LPRCore_agg service to effect the changes.

6.3.2 How Data from the Publisher Is Displayed By the Subscriber

- On the Data Mining pages, the remote server node name shows up in the **Reader** column.
- In case a Subscriber receives reads from a remote domain and some of the reads match a List on the Subscriber there will **NOT** be any local alarm because in our current system List matching is performed exclusively by CarSystem and not by the EOC webserver software.

7 Safe Mode

7.1 Safe Mode

Safe mode is a default system account that always allows you to log in, even if you've somehow broken your permissions in such a way that a regular administrative account will not login.

You must log into Safe Mode on the physical machine where the EOC resides (i.e., localhost).

Safe Mode is available regardless of whether you are operating in Active Directory Mode or SQL Server Mode.

When you log into Safe Mode, you will lock other users out of the EOC system for the duration of your session. Other users will see a splash screen with the message that the system is undergoing maintenance.

The login name for Safe Mode is: **SafeModeUser**; the default password is **SafeModeUser**. For obvious reasons, this user name and password cannot be changed.

7.1.1 Enter or Exit Safe Mode

Safe Mode can be accessed as described below.

(1) To log into the system in Safe Mode, go to the physical machine where the EOC server resides and navigate to the correct URL for the EOC server.

(2) Login to the EOC as a user with sufficient privileges to access **Application Settings**

(3) Navigate to **System > App Settings > Safe Mode**.

(4) Referring to Figure 61, click the **Enter Safe Mode** button.

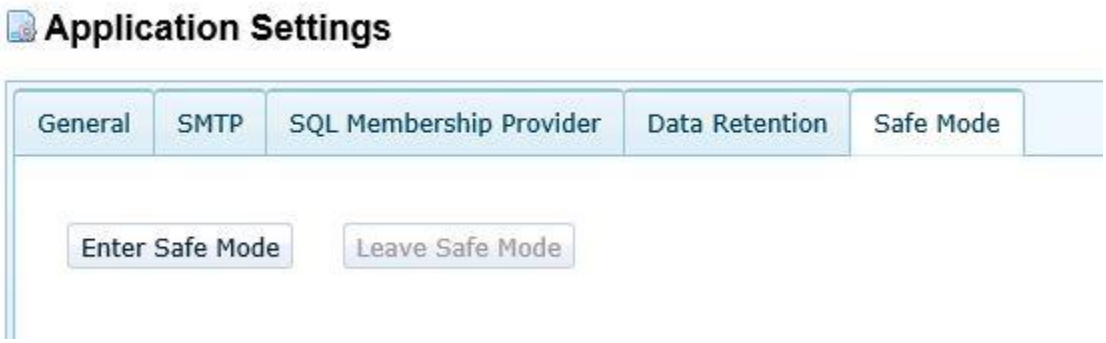

Figure 61 — System App Settings Safe Mode Selection

(5) Referring to Figure 62, click the **OK** button to confirm entering Safe Mode. Click the **Cancel** button to cancel entering Safe Mode

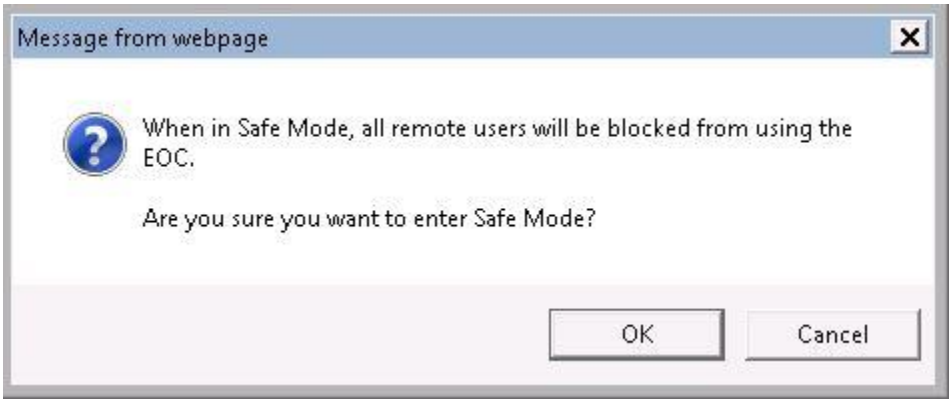

Figure 62 — Entering Safe Mode Warning Message

(6) Referring to Figure 63, you will automatically be logged in as SafeModeUser.

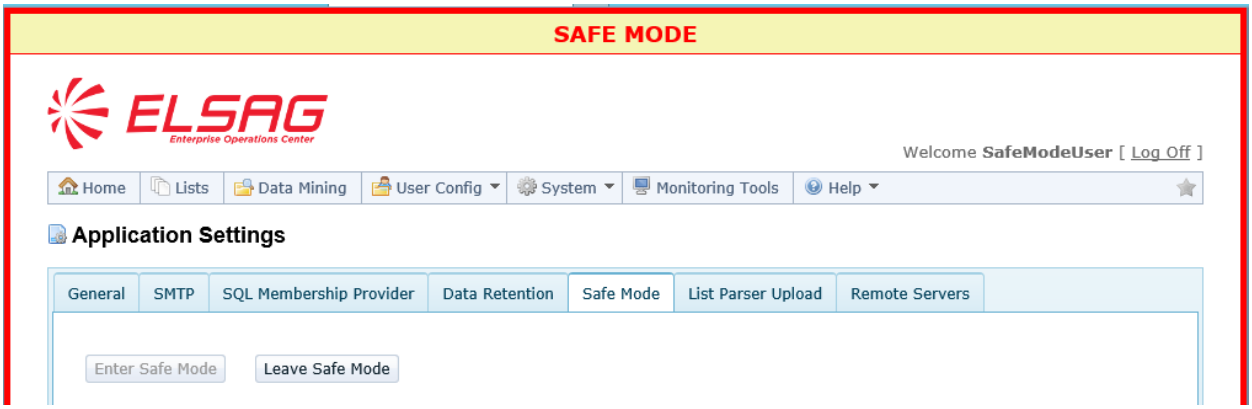

Figure 63 — EOC Safe Mode Enabled

(7) Now you can perform whatever maintenance or error correction you need to do.

(8) Referring to Figure 63, to log out of Safe Mode, navigate to **System > App Settings > Safe Mode**.

(9) Click the "**Leave Safe Mode**" button.

(10) Referring to Figure 64, click "OK" to confirm exiting Safe Mode. The EOC will exit Safe Mode and leave you at the log in screen.

Figure 64 — EOC Exit Safe Mode Confirmation Question

7.1.2 Safe Mode Session Timeout

Every EOC user session has a session timeout. That is, if you log into the EOC and get distracted and do not perform any actions for that long, your session times out and you are automatically logged out. At this point, you must log back into the EOC to do any work. For all users created using the **User Config > User Manager** page, the session timeout is configurable based upon the user's group membership. The default timeout is 30 minutes.

Note, however, that once you switch into Safe Mode, you will be logged in as SafeModeUser. This user cannot be added to any groups and so the session timeout will always be 30 minutes. So if you switch into Safe Mode and do not perform any actions for more than 30 minutes, your session will time out. At that point, you will have to log back into the NAS as SafeModeUser before you can leave Safe Mode. You will not be able to log in as any other user until you leave Safe Mode.

7.1.3 Membership Provider: SQL or Active Directory

Allows the user Membership Provider to be switched to or from SQL Server Mode from or to Active Directory Mode. If EOC is already in Active Directory Mode, you can review the Active Directory settings for Connection String, Network Domain and Username.

Follow these steps to change the EOC to Active Directory Mode:

(1) Follow the instructions for entering Safe Mode in *Enter or Exit Safe Mode* on page 79.

(2) Referring to Figure 65, navigate to the **System** > **App Settings** > **Safe Mode** tab.

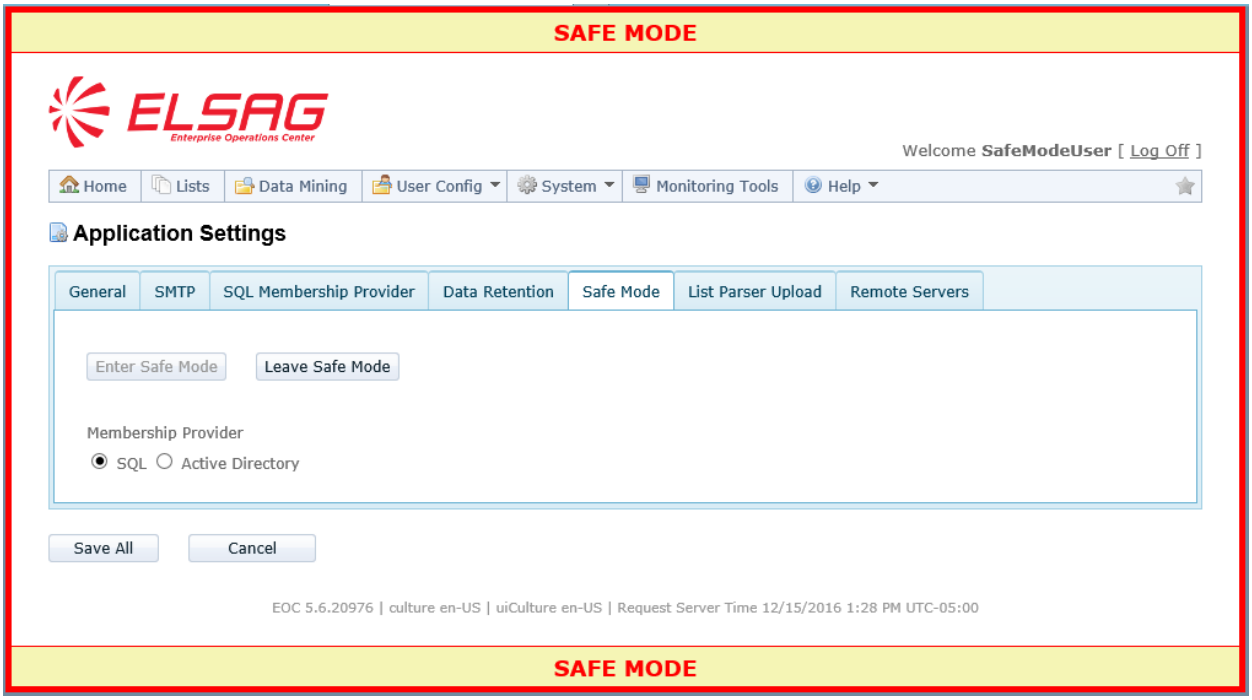

Figure 65 — Application Settings Safe Mode Tab

(3) Referring to Figure 66, select the Active Directory radio button which will display the fields needed to switch to Active Directory Mode.

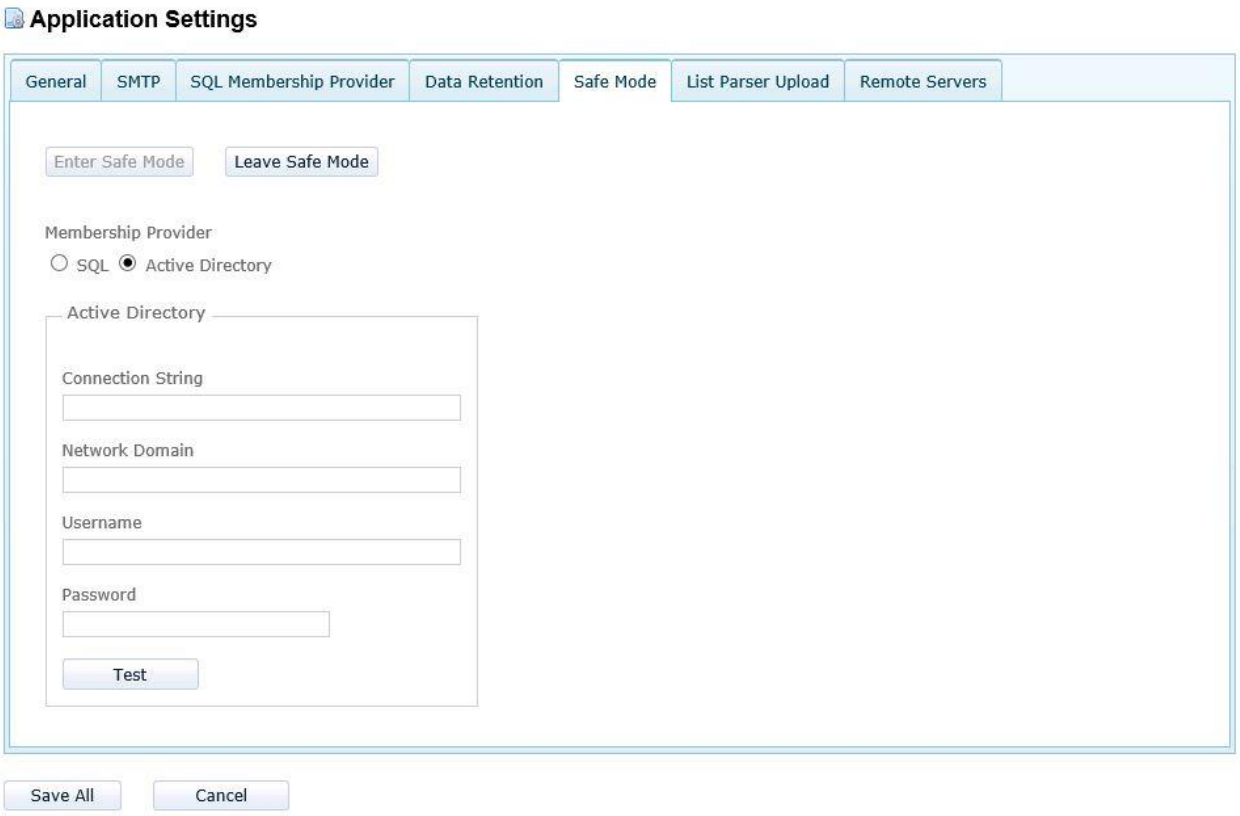

Figure 66 — Membership Provider Active Directory Entry

(4) Referring to Figure 67, enter the required information and click the **Test** button.

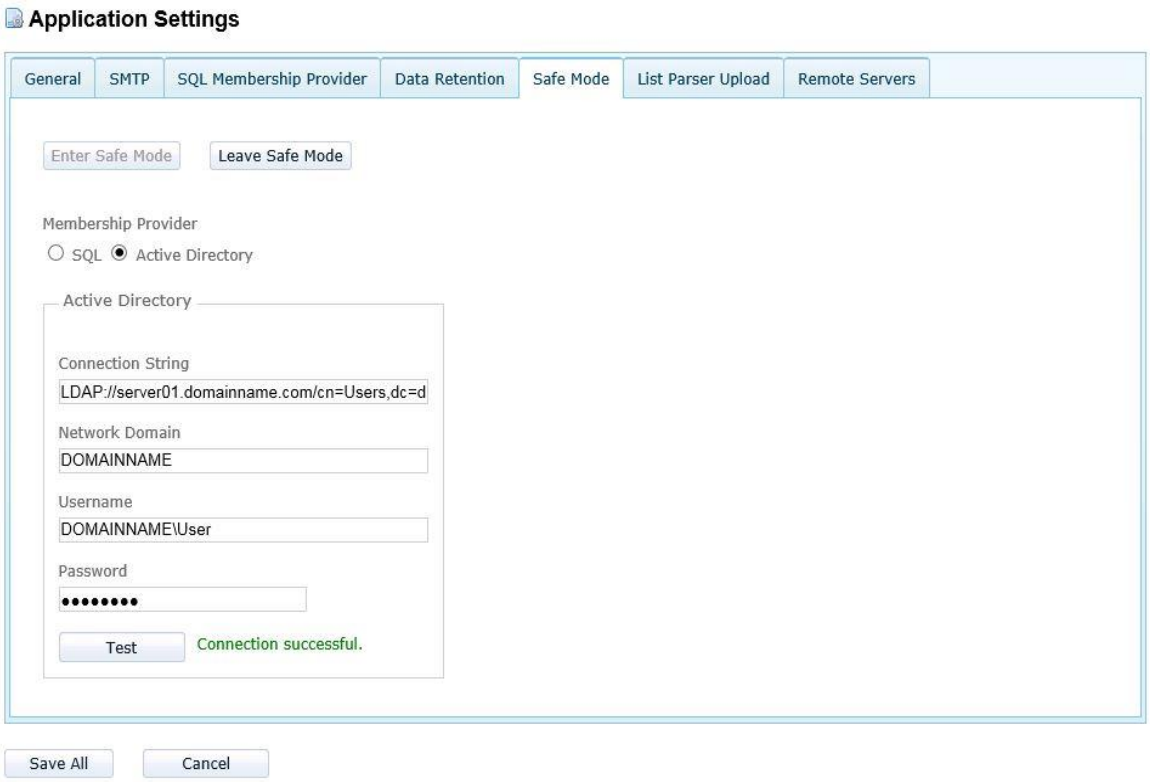

Figure 67 — Active Directory Test Successful

(5) Referring to Figure 67, if you receive the "**Connection Successful**" message click **Save All**. If the "**Connection Successful**" message is not displayed, make any corrections necessary to successfully test the settings.

NOTE: The **Save All** button saves changes to all Application Settings tabs at the same time.

(6) Referring to Figure 68, successfully saved Application Settings will display "The Application Settings have been successfully saved." message.

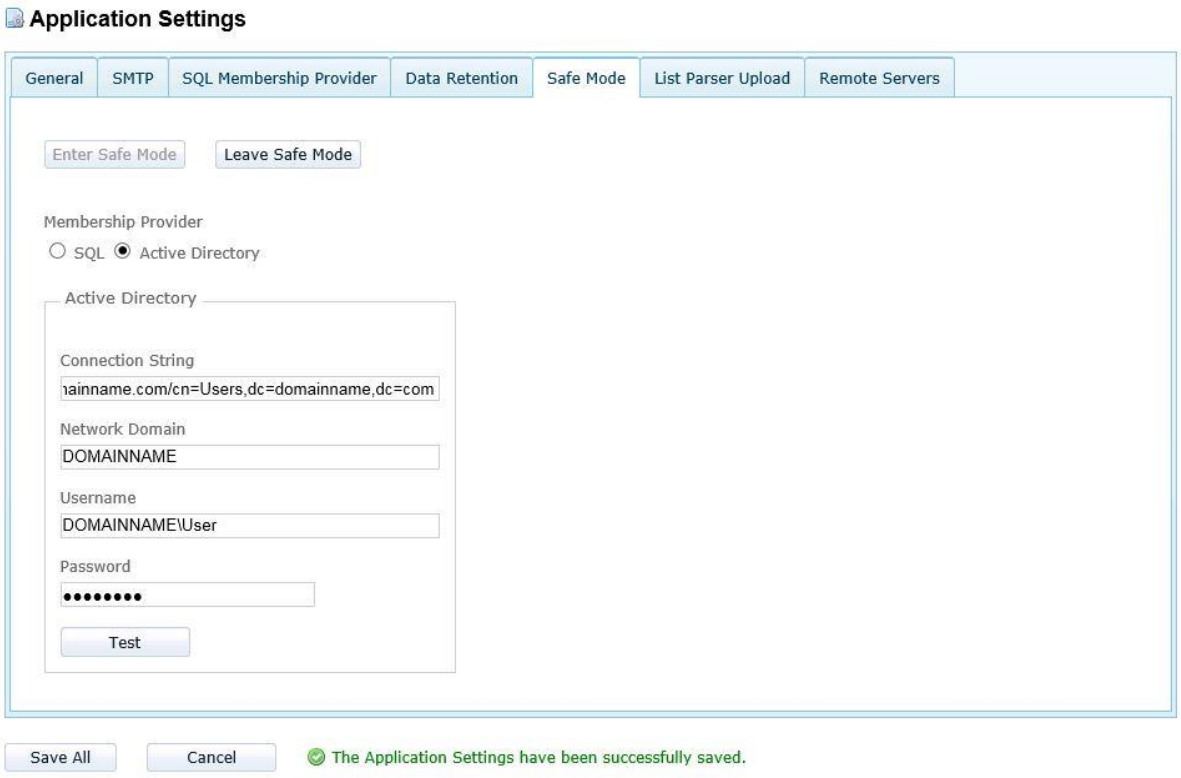

Figure 68 — Active Directory Settings Saved

(7) Referring to Figure 68, the complete the change to Active Directory, click the **Leave Safe Mode** button and acknowledge that you want to leave safe mode.

Figure 69 — Leave Safe Mode Confirmation

7.1.3.1 Changing from SQL Server Mode to Active Directory Mode

There are prerequisites for converting to Active Directory Mode, both for the EOC Server machine and for each CarSystem installation that will operate in Active Directory Mode.

7.1.3.1.1 EOC Server Side

- The LDAP Server must be hosted using Microsoft Active Directory.
- All EOC users must be in one LDAP directory tree.
- An LDAP connection string must be established, including host, port and protocol that points to the relevant Users container. For example:
  LDAP://ds1.example.com/CN=Users,DC=example,DC=com
- You must have an LDAP login username and password.
- Set firewall access to the LDAP server to either unencrypted connection on TCP/389 or Implicit SSL Encryption connection on TCP/636.

NOTE: Queries of the Global Catalog are not supported.

7.1.3.1.2 CarSystem Installations

Each CarSystem installation that will be used in Active Directory Mode must meet the following requirements:

- The CarSystem computer must be attached to the LDAP server's Active Directory domain or on a domain in the same domain forest. A trusted domain will also work.
- The user in CarSystem must have log in permission on the client computer.
- The CarSystem user must have either network access to the domain controller at login time or must be able to use cached credentials. (These are standard requirements for Windows Active Directory logins.)
- CarSystem will automatically authenticate using the credentials that the Active Directory user logged into Windows with or as a specific user when used with the **Run As...** command.

Once you've made sure that all the prerequisite software and IIS settings are correct on your computer, you can convert the EOC 5.x server to Active Directory Mode.

8 Communication Ports

8.1 Communication Port Information

The EOC and CarSystem components use certain default ports to communicate. EOCs configured for Data Sharing, both Copy Data and Search Data, use additional default ports.

8.1.1 Standard EOC Installation Communications

Figure 70 illustrates the components, the ports they use by default, and the direction in which communication is initiated for a standard EOC installation.

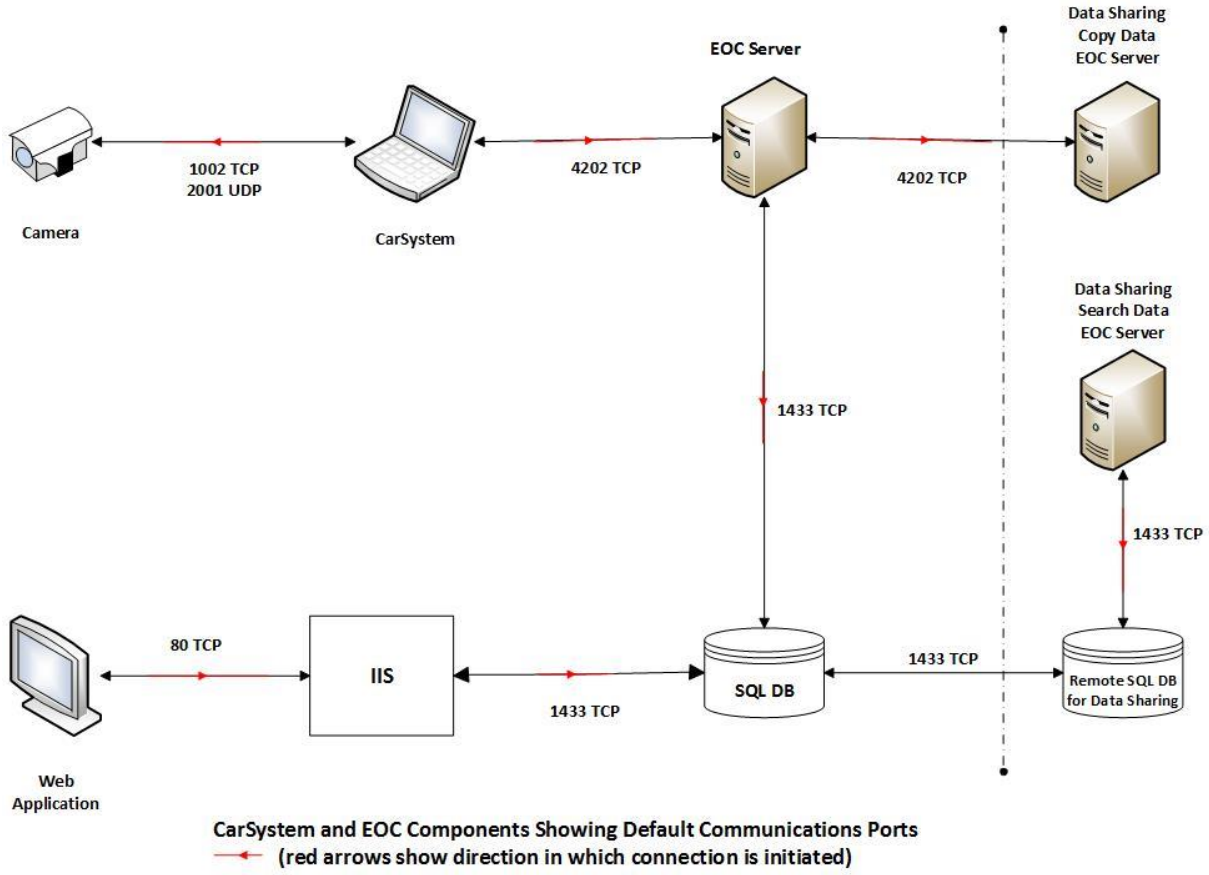

Figure 70 — Components, Ports, and Communications Direction

8.1.2 Split EOC Installation Communications

Figure 71 illustrates the components, the ports they use by default, and the direction in which communication is initiated for a split web server and aggregator EOC installation.

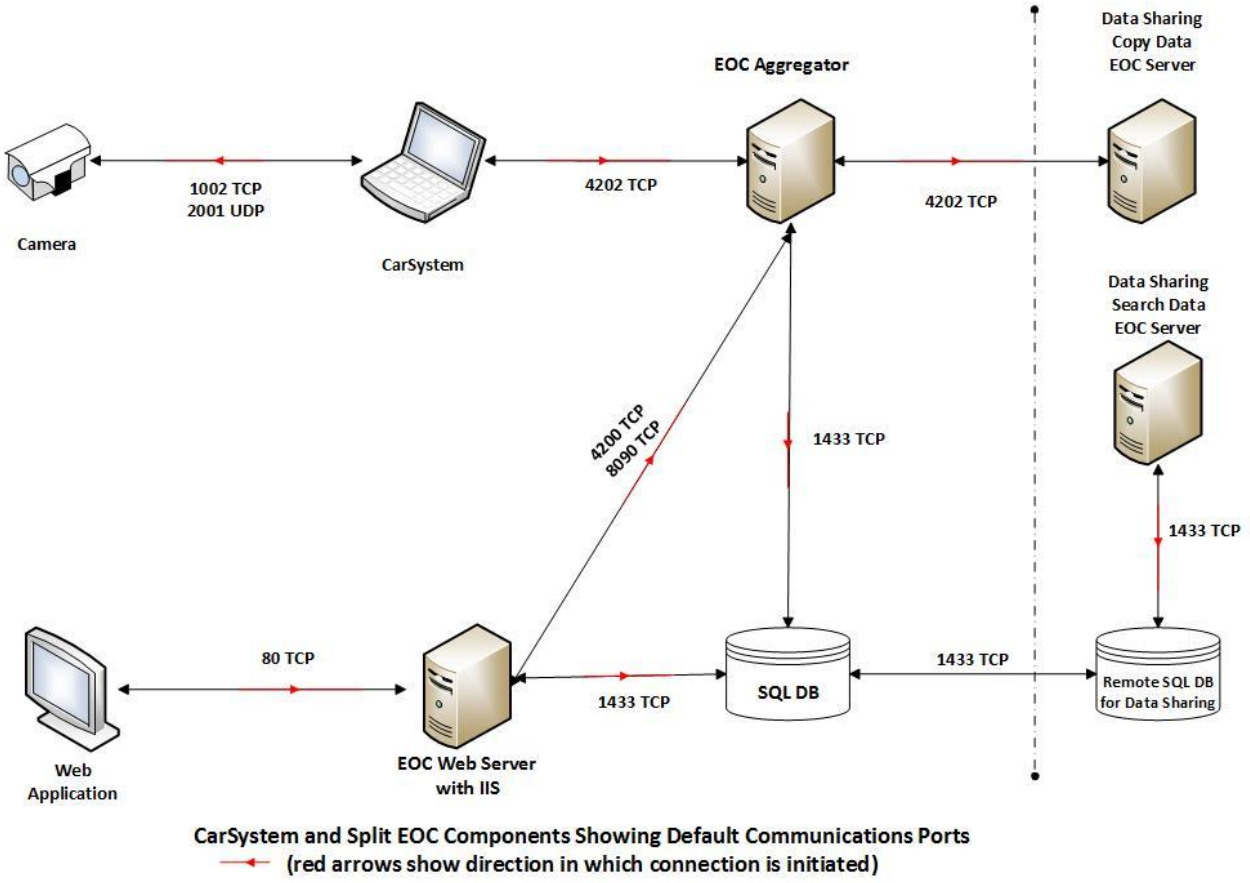

Figure 71 — Split EOC Installation Components, Ports, and Communications Direction

The same information is summarized below in Table J.

Table J — Components, Ports, and Communications Direction

Component and Path	Default Port(s)	Connection Direction
Camera to CarSystem	1002, 1004 TCP for data 2001 UDP for diagnostics	From CarSystem to Camera
CarSystem to/from EOC Server	4202 TCP for data	From CarSystem to EOC Server
Data Sharing Copy Data EOC Server to EOC server	4202 TCP for data	From Publisher EOC Server to Subscriber EOC Server
EOC Webserver to EOC Aggregator (Split install)	4200 TCP for data 8090 TCP for Dispatcher	From Webserver to Aggregator
EOC Server to/from SQL Server DB	1433 TCP	From EOC Server to SQL DB
EOC Web application to/from IIS	80 TCP for data	From Web application to IIS
IIS to/from SQL Server DB	1433 TCP	From IIS to SQL DB
Data Sharing Search Data SQL Server DB to/from Remote Server SQL Server DB	1433 TCP	Either direction

NOTE: The use of port 4200 between CarSystem and EOC server for diagnostics was discontinued after EOC 4.2.

8.2 Configuring Cameras

For information about how to configure the cameras' firmware, see the *Elsag Plate Hunter® CarSystem Installation Guide*, Publication Number MPH-900-CSIG.

The CarSystem installation process will normally configure and connect the cameras to the EOC automatically. To configure the cameras' connections to the EOC manually or to add a new camera or change camera names, see the *Elsag Plate Hunter® CarSystem User's Guide*, Publication Number MPH-900-CSUG.

NOTES:

NOTES:

NOTES:


ELSAG
a Leonardo Company